Name.com

DATA PROCESSING ADDENDUM (CUSTOMERS)

Last Revised: December 6, 2021

This Data Processing Addendum (the "Addendum") is executed by and between Name.com, a Delaware limited liability company and its Affiliates ("Name.com") and you ("Customer") and is, where necessary, deemed annexed to and supplements the Web Hosting Service Agreement and any and all agreements governing an Applicable Service (collectively, the "Terms of Service"). Unless otherwise defined this Addendum, all capitalized terms not defined in this Addendum will have the meanings given to them in the Terms of Service.

1. Definitions

"Affiliates" means any entity, which is controlled by, controls or is in common control with Name.com.

"Applicable Services" means the Name.com hosted services we offer you that could involve our Processing of Personal Data as provided by you, as Data Controller.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq. This shall include any amendments and any implementing regulations thereto that become effective on or after the effective date of this Data Processing Addendum.

"Customer Data" means the Personal Data of any Data Subject Processed by Name.com within the Name.com Network on behalf of Customer pursuant to or in connection with the Terms of Service.

"Data Controller" means the Customer i.e. the entity and/or person which determines the purposes and means of the Processing of Personal Data.

"Data Processor" means Name.com. i.e. the entity which Processes Personal Data on behalf of and on the instructions of the Data Controller, or as defined in other applicable legislation.

"Data Protection Laws" means all data protection or privacy laws and regulations applicable to the Processing of Personal Data under the Agreement, including, (i) the CCPA, (ii) the GDPR, (iii) the EU e-Privacy Directive (Directive 2002/58/EC), (iv) any national data protection laws made under or pursuant to (i) or (ii), (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance, and (vi), in respect of the United Kingdom the Data Protection Act 2018 and any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; in each case as may be amended, superseded or replaced.

"Data Subject" means the individual to whom Personal Data relates.

"EEA" means the European Economic Area.

"General Data Protection Regulation" or "GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Name.com Network” means Name.com’s service providers and their data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls), as applicable, which are used to provide the Applicable Services.

“Personal Data” means any information relating to an identified or identifiable person or household as defined under applicable Data Protection Laws.

“Privacy Shield” means Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176).

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, to include, but not limited to; collection, recording, organization, structuring, storage, security, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, rectification, erasure or destruction. “Process”, “processes” and “processed” will be interpreted accordingly. Details of Processing are set forth in Annex 1.

“Security Incident” either (a) a breach of security of the Name.com Technical and Organizational Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data; or (b) any unauthorized access to Name.com equipment or facilities, where in either case such access results in destruction, loss, unauthorized disclosure, or alteration of Customer Data.

“Technical and Organizational Measures” means the listed measures relating to the security of data at Name.com, attached to this Addendum as Annex 2.

“Standard Contractual Clauses” or “SCCs” means Annex 3, attached to and forming part of this Addendum pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive and any amendments or changes to any other law relating to data and privacy as may be amended, superseded or replaced.

“Sub-processor” means any Data Processor engaged by Processor to Process data on behalf of Data Controller under the Terms of Service.

2. Data Processing

A. **Scope and Roles.** This Addendum applies when Customer Data is processed by Name.com in the provision of Applicable Services under the Terms of Service. In this context, Name.com (Data Processor) shall only act on instructions of the Customer (Data Controller) with respect to Customer Data, unless directed by a legal or regulatory requirement by a competent body or authority.

B. **Details of Data Processing.** The subject matter of processing of Customer Data by Name.com is the performance of the Applicable Services pursuant to the Terms of Service and product-specific agreements. Name.com shall only Process Customer Data on behalf of and in accordance with Customer’s documented instructions (limited to those instructions as contained in the Terms of Service) for the following purposes:

i. Processing in accordance with the Terms of Service or applicable product-specific agreement;
ii. Processing initiated by customer in their use of the Applicable Services;
iii. Processing to comply with other documented, reasonable instructions provided by Customers where such instructions are consistent with the terms of the Agreement.

Name.com shall not:

a. process, retain, use, sell, or disclose Customer Data except as necessary to provide Applicable Services pursuant to the Terms of Service, or as required by law;
b. sell such Customer Data to any third party;
c. retain, use, or disclose such Customer Data outside of the direct business relationship between Name.com and Customer save as is required or permitted under applicable legislation.

For the avoidance of doubt, Customer's instructions for the Processing of Personal Data must comply with all applicable data privacy laws. Customer shall have sole responsibility to understand and be aware of all applicable data privacy laws for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Name.com shall not be required to comply with or observe Customer's instructions if such instructions would violate Data Protection Laws or any other applicable laws and legislation. The duration of the Processing, the nature and purpose of the Processing, the types of personal data and categories of Data Subjects Processed under this Addendum are set out in Annex 1 ('Details of the Processing') to this Addendum.

3. Confidentiality of Customer Data

A. Name.com will not disclose Customer Data to any government or any other third party, except as necessary to comply with our legal obligations, the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). In the event Name.com receives a valid civil subpoena, and to the extent permitted, Name.com will endeavor to provide Customer with reasonable notice of the demand via email or postal mail to allow Customer to seek a protective order or other appropriate remedy as they deem appropriate.

4. Security

A. Name.com has implemented and will maintain the technical and organizational measures for the Name.com Network as described herein this Section and as further described in Annex 2 to this Addendum, Security Standards. In particular, Name.com has implemented and will maintain these technical and organizational measures so as to address the:

i. security of the Name.com Network;
ii. physical security of the Name.com facilities;
iii. controls around employee and contractor access to i and/or ii; and
iv. processes for testing, assessing and evaluating the effectiveness of technical and organizational measures implemented by Name.com.

In the event that we are not able to meet any of our obligations set forth herein, we will endeavor to provide written notice (via our website and email) as soon as practically feasible.

B. Name.com makes available a number of security features and functionalities that Customer may elect to use in relation to the Applicable Services, including two-factor authentication for your Name.com account, as well as the ability to change and update your passwords, and Name.com account-level IP address access restrictions,. Customer is responsible for (a) properly configuring the Applicable Services, (b) using the controls available in connection with the Applicable Services (including the security controls) to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) using the controls available in connection with the Applicable Services (including the security controls) to allow the Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

5. Data Subject Rights

A. As sole Controller, all Data Subject Requests, as defined herein, are the responsibility of the Customer. As commercially reasonable, and to the extent lawfully required or permitted, Name.com shall endeavor to use best efforts to promptly notify Customer if Name.com directly receives a request from a Data Subject to exercise such rights under any applicable data privacy laws ("Data Subject Request"). In addition, where Customer's use of the Applicable Services limits its ability to address a Data Subject Request, Name.com may, where legally permitted and appropriate and upon Customer's specific request, provide commercially reasonable assistance in addressing the request, at Customer's cost (if any).

6. Sub-Processing

A. *Authorized Sub-processors*. Customer agrees that Name.com may use Sub-processors to fulfil its contractual obligations under its Terms of Service and this Addendum or to provide certain services on its behalf, such as providing support services. Customer hereby consents to Name.com's use of Sub-processors as described in this Section. Except as set forth in this Section or as otherwise explicitly authorized by you, Name.com will not permit any other sub-processing activities.

B. *Sub-processor Obligations.* Where Name.com uses any authorized Sub-processor as described in Section 6.A.:

i. Name.com will restrict the Sub-processor's access to Customer Data to only that what is necessary and required to maintain the Applicable Services or that which is necessary to provide the Applicable Services to Customer in accordance with the Applicable Services.

ii. Name.com will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is performing the same data processing services that are being provided by Name.com under this Addendum, the appointment of that subcontractor by Name.com shall be conditional on the sub-processor being subject to equivalent obligations envisaged under this Data Protection Addendum; and

iii. Name.com will remain responsible for its compliance with the obligations of this Addendum including any acts or omissions of the Sub-processor that cause Name.com to breach our obligations under this Addendum.

C. *Engaging New Sub-processors.* From time to time, Name.com may engage new Sub-processors in order to provide the Name.com services to Customer. In such case, we will endeavor to provide **60 days advance notice** (via our website and email) prior to any new Sub-processor obtaining any Customer Data.

i. If you, the Customer, do not approve of a new Sub-processor, then you may terminate any Applicable Services, without penalty, by providing Name.com, within 10 days of the issuance of the notice, a written notice of termination that must include an explanation of the reasons for your non-approval of the new Sub-processor.

ii. If the Applicable Services are part of a bundle or bundled purchase, then any termination will apply in its entirety.

7. Security Breach Notification

A. *Security Incident.* Where Name.com confirms that a Security Incident occurred, Name.com will, without undue delay:

i. notify Customer of the Security Incident in their capacity as Data Controller; and

ii. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

B. *Name.com Assistance*. To assist Customer in relation to any personal data breach notifications Customer is required to make under any applicable privacy laws, Name.com will include in the notification such information about the Security Incident as Name.com is reasonably able to disclose to Customer, taking into account the nature of the Applicable Services, the information available to Name.com, and any restrictions on disclosing the information, such as legal requirements and confidentiality.

C. *Failed Security Incidents*. Customer agrees that:

i. A failed Security Incident will not be subject to the terms of this Addendum. A failed Security Incident is one that results in no unauthorized access to Customer Data or to any of Name.com's Network, equipment, or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

ii. Name.com's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Name.com of any fault or liability of Name.com with respect to the Security Incident.

D. *Communication*. Notification(s) of Security Incidents, if any, will be delivered to Customers contact details as advised to us, including via email, or as requested. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the Name.com management console and secure transmission at all times.

8. Customer Rights

A. *Independent Determination.* Customer is responsible for reviewing the information made available by Name.com relating to data security and its Security Standards and making an independent determination as to whether the Applicable Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum. The information made available is intended to assist Customer in complying with Customer's obligations under applicable Data Protection Laws, including the GDPR and CCPA, in respect of data protection impact assessments and prior consultation.

B. *Audit Rights*. Upon Customer's request, and provided that the parties have an applicable non-disclosure agreement in place, Name.com will provide to Customer a list of administrative and technical controls utilized to ensure the protection of systems and data. Name.com will make this documentation available to Customer via secure file share and this documentation will be treated as Confidential Information under the applicable non-disclosure agreement. Additionally, such requests may only be made on an annual basis. If the requested audit scope is address in an SSAE 16/ISAE 2403 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's request and Name.com confirms there are no known material changes in the controls audited, the Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

9. Transfers of Personal Data

A. *U.S. Based Processing***.** Except where specifically noted in the Terms of Service, Customer Data is required to be transferred outside the EEA and processed in the United States to ensure that the Terms of Service can be fully implemented.

B. *Privacy Shield.* Name.com, as part of Donuts Inc., complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States in reliance on Privacy Shield. Transfers shall ordinarily be carried out in line with our undertakings and obligations under Privacy Shield; however, notwithstanding this, and in the event that Privacy Shield is considered not applicable or invalid, the Parties shall rely on the application of Standard Contractual Clauses, and any amendments or changes to any other law relating to data and privacy as may be amended, superseded or replaced (incorporated at Annex 3) . Where applicable, the Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an equivalent and adequate level of protection for Personal Data. The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply where the data is transferred in accordance with a recognized compliance standard for the lawful transfer of Personal Data outside the EEA, such as when necessary for the performance of Applicable Services pursuant to the Terms of Service or with your consent.

C. In all other circumstances for the avoidance of any doubt, the Customer shall undertake that the transfer is necessary for the conclusion or performance of a contract, concluded in the interest of the Data Subject, between the controller and the processor.

10. Termination of the Addendum

A. This Addendum will continue in force until the termination of our processing in accordance with the Terms of Service (the “Termination Date”).

11. Return or Deletion of Customer Data

A. As described in the Applicable Services, the Customer may be provided with controls that maybe used to retrieve or delete Customer Data. Any deletion of Customer Data will be governed by the terms of the particular Applicable Services and in accordance with applicable legislation.

12. Limitations of Liability

A. The liability of each party under this Addendum will be subject to the exclusions and limitations of liability set out in the Terms of Service. Customer agrees that any regulatory penalties incurred by Name.com in relation to the Customer Data that arise as a result of, or in connection with, Customer’s failure to comply with its obligations under this Addendum and any applicable Data Privacy Laws will be the sole responsibility of Customer and will count towards and reduce Name.com’s liability under the Terms of Service as if it were liability to the Customer under the Terms of Service.

13. Entire Terms of Service; Conflict

A. This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and Name.com, whether written or oral, regarding the subject matter of this Addendum, including any data processing addenda entered into between Name.com and Customer with regard to the processing of personal data and on the free movement of such data. Except as amended by this Addendum, the Terms of Service will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Terms of Service and this Addendum, the terms of this Addendum will control.

Annex 1

TYPES OF PROCESSING

1. Nature and Purpose of Processing. Name.com will Process Personal Data as necessary to perform the Applicable Services pursuant to the Terms of Service, product-specific agreements, and as further instructed by Customer throughout its use of the Applicable Services.

2. Duration of Processing. Subject to Section 10 of this Addendum, Name.com will Process Personal Data from the effective date of the Terms of Service, but will abide by the terms of this Addendum for the duration of the Processing if in excess of that term, and unless otherwise agreed upon in writing.

3. Categories of Data Subjects. Customer may upload Personal Data in the course of its use of the Applicable Services, the extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Prospects, customers, business partners and vendors of Customer (who are natural persons).

Employees or contact persons of Customer's prospects, customers, business partners and vendors.

Employees, agents, advisors, freelancers of Customer (who are natural persons).

Customer's Users authorized by Customer to use the Applicable Services.

4. Type of Personal Data. Customer may upload Personal Data in the course of its use of the Applicable Services, the type of and extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data of Data Subjects:

Name

Address

Telephone number

Date of birth

Email address

Other data collected that could directly or indirectly identify you or other any other Data Subject.

** **

Annex 2

TECHNICAL AND ORGANIZATIONAL MEASURES

1. Technical and Organizational Measures

We are committed to protect our customers' information. Taking into account the best practices, the costs of implementation and the nature, scope, circumstances and purposes of processing as well as the different likelihood of occurrence and severity of the risk to the rights and freedoms of natural persons we have implemented the following technical and organizational measures. When selecting the measures the confidentiality, integrity, security, availability and resilience of the systems are evaluated. A quick and efficient recovery after a physical or technical incident is a priority requirement we endeavor to complete.

The following technical and organizational measures are in place as relates to Name.com owned and operated infrastructure:

a. Information security policies;
b. Security awareness training for all applicable employees;
c. Physical security measures, including limited authorized access and access logging;
d. Detection and response measures;
e. Company-wide Document Retention Policy;
f. Patch and vulnerability management;
g. Role-based access control systems; and
h. Incident management.

2. Data Privacy Program

Our chosen partners, listed below, have established and maintain, a global data governance structure and secure information throughout its lifecycle. Where we engage third parties hosting providers, we will ensure there are adequate data processing agreement and procedures in place to ensure the security of your data. We regularly assess and evaluate or test the effectiveness of their Data Privacy Program and Security Standards by reviewing and confirming that our partners industry security certifications (SOC 2 Type, ISO 27001, etc.) are in compliance annually.

Our partners use a variety of physical and logical measures to protect the confidentiality of customer personal data. Those measures can be found here: https://www.ibm.com/support/customer/csol/terms/?cat=data-security#detail-document.

Annex 3

Standard Contractual Clauses (processors) (See Section 9.B. for applicability of these SCCs)

ANNEX 3

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

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)[1] 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 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

[1] 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 of 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 […].

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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 dataexporter 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 organisationalmeasures, to satisfy its obligations under these Clauses.

~~MODULE ONE: Transfer controller to controller~~

~~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 withoutundue 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[2] of the data and all back-ups at the end of the retention period.~~

~~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 personaldata 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 whommore 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.~~

~~[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.~~

~~(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.~~

~~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[3] (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.~~

~~[3] 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.~~

~~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.~~

~~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.~~

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, thedata importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties 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 subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose ofprocessing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subjectshall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate itspossible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available tothe data importer.

8.7 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 and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

[4] 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) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out withreasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

~~MODULE THREE: Transfer processor to processor~~

~~8.1 Instructions~~

~~(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.~~

~~(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.~~

~~(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.~~

~~(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].~~

~~[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.~~

~~8.2 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., unless on further instructions from the controller, ascommunicated to the data importer by the data exporter, or from the data exporter.~~

~~8.3 Transparency~~

~~On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter 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.~~

~~8.4 Accuracy~~

~~If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.~~

~~8.5 Duration of processing and erasure or return of data~~

~~Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, thedata importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).~~

~~8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.~~

~~(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.~~

~~(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.~~

~~(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.~~

~~8.7 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 and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.~~

~~8.8 Onward transfers~~

~~The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union~~[6]

[6] ~~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~~

~~(in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:~~

~~(i) the onward transfer 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;~~

~~(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or~~

~~(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.~~

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

~~8.9 Documentation and compliance~~

~~(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.~~

~~(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.~~

~~(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, whichshall provide it to the controller.~~

~~(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.~~

~~(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.~~

~~(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out withreasonable notice.~~

~~(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.~~

~~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 purposes of these Clauses.~~

~~MODULE FOUR: Transfer processor to controller~~

~~8.1 Instructions~~

~~(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.~~

~~(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.~~

~~(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.~~

~~(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.~~

~~8.2 Security of processing~~

~~(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data[7], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption orpseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.~~

~~(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware ofit and assist the data importer in addressing the breach.~~

~~(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.~~

~~8.3 Documentation and compliance~~

~~(a) The Parties shall be able to demonstrate compliance with these Clauses.~~

~~[7] This includes whether the transfer and further processing 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.~~

~~(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.~~

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

~~(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub- processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.~~

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least ***60 days*** in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

~~MODULE THREE: Transfer processor to processor~~

~~(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specificauthorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.~~

~~OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).~~

~~(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.~~

~~(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.~~

~~(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.~~

~~(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the~~

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

~~sub-processor contract and to instruct the sub-processor to erase or return the personal data.~~

Clause 10

Data subject rights

~~MODULE ONE: Transfer controller to controller~~

~~(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.[10] 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 todo so under the laws of the country of destination, provided that such laws lays downsuitable 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:~~

[10] ~~That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.~~

~~(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 thereequest.~~

~~(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.~~

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

~~**MODULE THREE: Transfer processor to processor**~~

~~(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.~~

~~(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.~~

~~(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the dataexporter.~~

~~MODULE FOUR: Transfer processor to controller~~

~~The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.~~

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[11] 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.~~]~~

~~MODULE ONE: Transfer controller to controller~~

MODULE TWO: Transfer controller to processor

~~MODULE THREE: Transfer processor to processor~~

(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 issueamicably 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 (EU) 2016/679.

[11] 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.

(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

~~**MODULE ONE: Transfer controller to controller**~~

~~**MODULE FOUR: Transfer processor to controller**~~

~~(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.~~

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

(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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

~~**MODULE ONE: Transfer controller to controller**~~

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

(a) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant toArticle 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competentsupervisory 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

Clause 14

Local laws and practices affecting compliance with the Clauses

~~**MODULE ONE: Transfer controller to controller**~~

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

~~**MODULE FOUR: Transfer processor to controller**~~ ~~*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*~~

(a) 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; theeconomic 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[12];

[12] 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

(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). ~~[For Module Three: The data exporter shall forward the notification to the controller.]~~

(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 to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation ~~[for Module Three: , if appropriate in consultation with the controller]~~. 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 ~~[for Module Three: the controller or]~~ 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

~~MODULE ONE: Transfer controller to controller~~

MODULE TWO: Transfer controller to processor

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.

~~**MODULE THREE: Transfer processor to processor**~~

~~**MODULE FOUR: Transfer processor to controller** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*~~

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.

~~[For Module Three: The data exporter shall forward the notification to the controller.]~~

(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.

~~(c)~~ 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 thecontract, 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.). ~~[For Module Three: The data exporter shall forward the information to the controller.]~~

(d) 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.

(e) 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 dataimporter 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~~. [For Module Three: The data exporter shall make the assessment available to the controller.]~~

(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 ~~[for ModuleThree: and the controller]~~ of such non-compliance. Where the contract involves morethan 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)~~ [For Modules ~~One,~~ Two ~~and Three~~: 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.] ~~[For Module Four: Personal data~~

~~collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.]~~ 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

~~**MODULE ONE: Transfer controller to controller**~~

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

[OPTION 1: 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 Republic of Ireland ~~(*specify Member State*).]~~

~~[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of________(*specify Member State*).~~]

~~**MODULE FOUR: Transfer processor to controller**~~

~~These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of________(*specify country*).~~

Clause 18

Choice of forum and jurisdiction

~~**MODULE ONE: Transfer controller to controller**~~

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

(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 Republic of Ireland ~~(*specify Member State*).~~

(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.

~~MODULE FOUR: Transfer processor to controller~~

~~Any dispute arising from these Clauses shall be resolved by the courts of_______(*specify country*).~~

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

~~MODULE ONE: Transfer controller to controller~~

MODULE TWO: Transfer controller to processor

~~MODULE THREE: Transfer processor to processor~~

~~MODULE FOUR: Transfer processor 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]*

SEE SIGNATORY OF AGREEMENT

Role (controller/processor): CONTROLLER (Customer)

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

SEE SIGNATORY OF AGREEMENT

Role (controller/processor): PROCESSOR (Name.com)

B. DESCRIPTION OF TRANSFER

~~MODULE ONE: Transfer controller to controller~~

MODULE TWO: Transfer controller to processor

~~MODULE THREE: Transfer processor to processor~~

~~MODULE FOUR: Transfer processor to controller~~

SEE Annex 1 of the Addendum

C. COMPETENT SUPERVISORY AUTHORITY

~~MODULE ONE: Transfer controller to controller~~

MODULE TWO: Transfer controller to processor

~~MODULE THREE: Transfer processor to processor~~

Identify the competent supervisory authority/ies in accordance with Clause 13

Office of the Data Protection Commissioner.
Canal House, Station Road, Portarlington, Co. Laois, R32 AP23, Ireland.
Phone +353 (0761) 104 800 | LoCall 1890 25 22 31 | Fax +353 57 868 4757
Email info@dataprotection.ie

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

~~**MODULE ONE: Transfer controller to controller**~~

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

See Annex 2 of the Addendum

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

~~**MODULE THREE: Transfer processor to processor**~~

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

As per Annex 3 of the Addendum

Annex 4

List of Sub-Processors

IBM