DATA PROCESSING AGREEMENT

This Data Processing Agreement (this “DPA”) is entered into as of March 1, 2024 (the “Effective Date”) between the following parties (each a “Party” and, collectively, the “Parties”).

G Treasury SS, LLC, a Delaware USA limited liability company (“GTreasury”)
2100 E Lake Cook Road - Suite 1100
Buffalo Grove, IL 60089 USA
Attention: Chief Financial Officer
Fax: (847) 847-3716
E-mail: accounting@gtreasury.com

<Customer>, a <Delaware> Limited Liability Company(“Customer”)
2100 East Lake Cook Road, Buffalo Grove, Illinois 60089, United States

123-4567-8901
[counterpartySignerEmail_mc5zbn9]

This DPA states obligations of GTreasury with respect to Covered Personal Data.

1. **Defined Terms.** Without limiting anything else in this DPA, the following terms will have the following meanings. Where this DPA defines a term, the definition applies with respect to this DPA and, except as otherwise stated in this DPA, this DPA does not modify any defined term, as such, in any other agreement that refers to this DPA.

(a) An “Affiliate” of, or a person “Affiliated” with, a specific person is a person that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, the person specified where “control,” including the terms “controlling,” “controlled by” and “under common control with,” means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting shares, by contract, or otherwise and “person” means an individual, a corporation, a partnership, a limited liability company, an association, a joint-stock company, a business trust, unincorporated organization, or unit of government.

(b) “Covered Personal Data” is Personal Data that:

(i) GTreasury receives from Customer or any third party (including, but not limited to, any Data Subject) within the scope one or more Underlying Agreements; and

(ii) Is protected by Data Protection Law and with respect to which Data Protection Law imposes protections because of its personal nature.

(c) “Data Protection Law” means international, national, state, or provincial law that protects, or imposes restrictions on Processing of, the Personal Data in question. The term includes, but is not limited to, the following, as amended, and the rules thereunder having the force of law, all to the extent that they meet the preceding definition: the General Data Protection Regulation (Regulation (EU) 2016/679) (the “GDPR”), the Australian Privacy Act 1988, the New Zealand Privacy Act 2020, Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”), the Swiss Federal Act on Data Protection, the UK Data Protection Act 2018, California Consumer Privacy Act of 2018 (“CCPA”), and the California Privacy Rights Act of 2020 (“CPRA”).

(d) A “Data Subject” with respect to Personal Data is the identified or identifiable natural person to which Personal Data relates.

(e) “EEA Personal Data” means Covered Personal Data whose Data Subjects are in the EEA.

(f) The “European Union,” or “EU,” means the member states of that union as established under the Treaty on European Union, the Treaty on the Functioning of the European Union, and related treaties, as such member states may accede or exit.

(g) The “European Economic Area” or “EEA” means the acceding member states under the European Economic Area Agreement, as such member states may accede or exit.

(h) “Personal Data” means any information relating to an identified or identifiable natural person, where an “identifiable natural person” is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(i) “Processing” of Personal Data means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(j) “Underlying Agreement” means an agreement between Customer and GTreasury under which GTreasury provides goods, services, and/or software to Customer.

2. **Generally.**

(a) Customer will not provide to GTreasury any Personal Data that is not necessary for the performance by GTreasury of GTreasury’s obligations under any Underlying Agreement.

(b) GTreasury’s obligations under this DPA apply to the extent that Data Protection Law that applies to Customer requires that Customer impose such obligations on processors of Covered Personal Data.

(c) GTreasury will not engage another processor without prior specific or general written authorization of Customer. In the case of general written authorization, GTreasury will inform Customer of any intended changes concerning the addition or replacement of other processors and give to Customer the opportunity to object to such changes.

(d) The subject matter, nature, and purpose of the Processing by GTreasury is the delivery of the goods, services, and/or software identified in the Underlying Agreement(s).

(e) The type of Personal Data and categories of Data Subjects are the types and categories contemplated by the Underlying Agreement(s).

(f) GTreasury will Processes Covered Personal Data only on documented instructions from Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Data Protection Law to which GTreasury is subject. In such a case, the GTreasury will inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest contemplated by Data Protection Law. For the avoidance of doubt, the Underlying Agreement constitutes Customer's documented instructions to GTreasury to perform such Processing as is necessary for GTreasury to perform under the Underlying Agreement.

(g) GTreasury will ensure that its agents authorized to process the Covered Personal Data have committed themselves to confidentiality or are under an appropriate statutory or professional obligation of confidentiality.

(h) Security.

(i) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, GTreasury will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, to the extent necessary and appropriate:

(A) Pseudonymisation and encryption of Covered Personal Data;

(B) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(C) The ability to restore the availability and access to Covered Personal Data in a timely manner in the event of a physical or technical incident; and/or

(D) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

(ii) In assessing the appropriate level of security, GTreasury will take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

(iii) GTreasury may use adherence to an approved code of conduct contemplated by GDPR Article 40 or an approved certification mechanism as contemplated by GDPR Article 42 as an element by which to demonstrate compliance with the requirements identified in Section 2(h)(i).

(iv) GTreasury will take steps to ensure that any natural person acting under the authority of GTreasury processor who has access to Covered Personal Data does not Process Covered Personal Data except on instructions from Customer unless he or she is required to do so by applicable Data Protection Law.

(i) GTreasury will not engage or use any third party to perform any Processing other than as provided for in this DPA. For the avoidance of doubt, GTreasury may use hosting services provided by Microsoft Corporation, Amazon Web Services, Inc., Rackspace, Inc., and/or or their affiliates, provided only that GTreasury obtains from such provider(s) contractual obligations consistent with GTreasury's performance of its obligations under this DPA.

(j) Taking into account the nature of the Processing, GTreasury will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's or Customer's controller's obligations to respond to requests for exercising the data subject's rights laid down in:

(i) GDPR Chapter III, in particular Articles 12 (Transparent information, communication, and modalities for the exercise of the rights of the data subject), 13 (Information to be provided where personal data are collected from the data subject), 14 (Information to be provided where personal data have not been obtained from the data subject), 15 (Right of access by the data subject), 16 (Right to rectification), 17 (Right to erasure ("right to be forgotten")), 18 (Right to restriction of processing), 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing), 20 (Right to data portability), 21 (Right to object and automated individual decision-making), 22 (Automated individual decision-making, including profiling), and 23 (Restrictions); and/or

(ii) Other applicable Data Protection Law.

(k) GTreasury will assist Customer in ensuring compliance with the obligations under GDPR Articles 32 (Security of processing), 33 (Notification of a personal data breach to the supervisory authority), 34 (Communication of a personal data breach to the data subject). 35 (Data protection impact assessment), and 36 (Prior consultation), and other applicable Data Protection Law; taking into account the nature of Processing and the information available to GTreasury.

(l) At Customer's option, GTreasury will delete or return all Covered Personal Data to Customer after the end of the provision of services relating to Processing and delete existing copies unless applicable law requires continued retention by GTreasury of the Covered Personal Data.

(m) GTreasury will make available Customer all information necessary to demonstrate compliance with the obligations in GDPR Article 28 and similar obligations under other Data Protection Law, and allow for, and contribute to, audits, including inspections, conducted by Customer or another auditor mandated by Customer. GTreasury will immediately inform Customer if, in GTreasury's opinion, an instruction violates Data Protection Law.

(n) If GTreasury engages a third party for carrying out specific Processing activities on behalf of, or for the benefit of, Customer, data protection obligations consistent with GTreasury's performance of its obligations set out in this DPA and the Underlying Agreement(s) will be imposed on that third party by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of applicable Data Protection Law. Where that third party fails to fulfil its data protection obligations, the GTreasury will remain fully liable to Customer for the performance of such obligations.

3. United States-Specific Provisions.

(a) **California**. The following provisions apply to transfers from Customer to GTreasury of Covered Personal Data that is subject to the California Consumer Privacy Act of 2018 (Cal. Civ. Code § Section 1798.100 et. seq.) ("CCPA") and the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 et. seq.) ("CPRA"), each as amended ("California Covered Personal Data"), to the extent that Customer is a" business" and GTreasury acts as a "service provider" with respect to California Covered Personal Data.

(i) GTreasury Processes California Covered Personal Data as a service provider.

(ii) Customer is disclosing California Covered Personal Data to GTreasury in connection with the Underlying Agreement(s) only for the limited and specified purposes of receiving the services under the Underlying Agreement(s).

(iii) GTreasury will retain, use, disclose, or otherwise Process California Covered Personal Data solely for the specific purpose of providing the services under the Underlying Agreement(s) or as otherwise required by law.

(iv) GTreasury will not:

(A) Retain, use, disclose, or otherwise Process California Covered Personal Data except as necessary to provide services under the Underlying Agreement(s) or as otherwise required by law;

(B) Sell California Covered Personal Data; or

(C) Share California Covered Personal Data other than as required in order to perform under the Underlying Agreement(s).

(v) GTreasury will cooperate with any reasonable and appropriate audits, inspections, or other steps that Customer is required by California law to perform to confirm that GTreasury Processes California Covered Personal Data in a manner consistent with GTreasury's obligations under this DPA.

(vi) GTreasury will promptly notify Customer if GTreasury can no longer comply with GTreasury's obligations under this DPA.

(vii) GTreasury will cooperate with Customer in responding and implementing verifiable consumer requests to exercise rights afforded to consumers by California law, including by assisting with appropriate technical and organizational measures. GTreasury will deliver to Customer, within five business days, any requests by consumers to exercise a right under California law, whether received from a consumer or an authorized agent, if the requestor's Personal Data is found within the California Covered Personal Data.

(viii) Upon written request by Customer or termination of the Agreement, GTreasury will promptly delete all California Covered Personal Data.

(ix) GTreasury will not Process California Covered Personal Data to create deidentified data without first obtaining authorization from Customer. In the event GTreasury is properly authorized, GTreasury will:

(A) Adopt reasonable measures to prevent deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(B) Maintain and use deidentified data in a deidentified form and to not attempt to re-identify the deidentified data, except that GTreasury may attempt to re-identify the information solely or the purpose of determining whether its deidentification processes satisfy the requirements of California law; and

(C) Contractually require any recipients of the deidentified data, including subprocessors, contractors, and other third parties, to comply with obligations consistent with GTreasury's obligations under this DPA.

(D) Remain fully liable for any failure by GTreasury or its employees, agents, or contractors to comply with GTreasury's obligations with respect to deidentified data.

(b) **Colorado**. On and after 1 July 2023, the following provisions apply to transfers from Customer to GTreasury of Covered Personal Data and Processing of Covered Personal Data by GTreasury that is subject to the Colorado Privacy Act, (Col. Rev. Stat. § 6-1-1301 et seq.), as amended ("Colorado Covered Personal Data") to the extent that Customer acts as a controller of Colorado Covered Personal Data and GTreasury acts as a Processor of the Colorado Covered Personal Data:

(i) GTreasury Processes Colorado Covered Personal Data as a processor when providing the services under the Underlying Agreement(s).

(ii) GTreasury will:

(A) Retain, use, disclose, or otherwise Process Colorado Covered Personal Data solely for the specific purpose of providing the services under the Underlying Agreement(s) or as otherwise required by law;

(iii) Ensure that each agent of GTreasury that Processes Colorado Covered Personal Data is subject to a duty of confidentiality with respect to the Covered Colorado Personal Data; and

(iv) To the extent that Customer is required by Colorado law to require the following of GTreasury:

(A) GTreasury will allow, and cooperate with, reasonable assessments by Customer or Customer's designated assessor; or

(B) GTreasury may arrange for a qualified and independent assessor to conduct an assessment of GTreasury's policies and technical and organizational measures using an appropriate and accepted control standard or framework and assessment procedure for such assessments and GTreasury will provide a report of such assessment to Customer upon request.

(v) At Customer's direction, GTreasury will delete or return all Colorado Covered Personal Data to Customer as requested at the end of the provision of services, unless retention of the Colorado Covered Personal Data is required by law;

(vi) Upon Customer's reasonable request, GTreasury will make available to Customer all information in its possession reasonably necessary to demonstrate GTreasury's compliance with this DPA;

(vii) GTreasury will cooperate with Customer by appropriate technical and organizational measures, insofar as this is reasonably practicable, in fulfilling Customer's obligation to respond to consumer rights requests. GTreasury will deliver to Customer, within five business days any request by a Data Subject to exercise a right under Colorado law, whether received from a Data Subject or an authorized agent, if the requestor's Covered Personal Data is found within Colorado Covered Personal Data.

(viii) GTreasury will assist Customer in meeting its obligations in relation to the security of processing Colorado Covered Personal Data and in relation to the notification of a breach of security of the system of GTreasury pursuant to applicable law.

(ix) GTreasury will not Process Colorado Covered Personal Data to create deidentified data without first obtaining authorization from Customer. In the event GTreasury is properly authorized, GTreasury will:

(A) Adopt reasonable measures to prevent deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; and

(B) Contractually require any recipients of the deidentified data, including subprocessors, contractors, and other third parties, to comply with obligations consistent with GTreasury's obligations under this DPA.

(c) **Virginia**. The following provisions apply to all transfers from Customer to GTreasury of Covered Personal Data and Processing of Covered Personal Data by GTreasury that is subject to the Virginia Consumer Data Protection Act (Va. Code § 59.1-571 et seq.) as amended ("VCDPA") ("Virginia Covered Personal Data") to the extent that Customer acts as a Controller of Virginia Covered Personal Data and GTreasury acts as a Processor of the Virginia Covered Personal Data.

(i) GTreasury Processes Virginia Covered Personal Data as a Processor when providing the services under the Underlying Agreement(s).

(ii) GTreasury will retain, use, disclose, or otherwise Process Virginia Covered Personal Data solely for the specific purpose of providing the services under the Underlying Agreement(s) or as otherwise required by law.

(iii) GTreasury will Ensure that each GTreasury agent processing Virginia Covered Personal Data is subject to a duty of confidentiality with respect to the data.

(iv) To the extent that Customer is required by Virginia law to require the following of GTreasury:

(A) GTreasury will allow, and cooperate with, reasonable assessments by Customer or Customer's designated assessor; or

(B) GTreasury may arrange for a qualified and independent assessor to conduct an assessment of GTreasury's policies and technical and organizational measures using an appropriate and accepted control standard or framework and assessment procedure for such assessments and GTreasury will provide a report of such assessment to Customer upon request.

(v) At Customer's direction, GTreasury will delete or return all Virginia Covered Personal Data to Customer as requested at the end of the provision of services, unless retention of the Virginia Covered Personal Data is required by law.

(vi) Upon Customer's reasonable request, GTreasury will make available to Customer all information in its possession necessary to demonstrate GTreasury's compliance with GTreasury's obligations under this DPA.

(vii) GTreasury will cooperate with Customer, by appropriate technical and organizational measures, insofar as this is reasonably practicable, in fulfilling Customer's obligation to respond to Data Subject rights requests. GTreasury will deliver to Customer, within five business days, any requests to exercise a right under Virginia Data Protection Law, whether received from a Data Subject or an authorized agent, if the requestor's Personal Data is found within the Virginia Covered Personal Data.

(viii) GTreasury will assist to assist Customer in meeting its obligations in relation to the security of Processing the Virginia Covered Personal Data and in relation to the notification of a breach of security of the system of GTreasury to the extent required by Virginia law.

(ix) GTreasury will not Process Virginia Covered Personal Data to create deidentified data without first obtaining authorization from Customer. In the event GTreasury is properly authorized, GTreasury will:

(A) Adopt reasonable measures to prevent deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(B) Maintain and use deidentified data in a deidentified form and to not attempt to re-identify the deidentified data, except that GTreasury may attempt to re-identify the information solely or the purpose of determining whether its deidentification processes satisfy the requirements of Virginia law; and

(C) Contractually require any recipients of the deidentified data, including subprocessors, contractors, and other third parties, to comply with obligations consistent with GTreasury's obligations under this DPA.

4. **Canada-Specific Provisions**. The following provisions apply to all transfers from Customer to GTreasury of Covered Personal Data, the Processing of which is subject

to the Personal Information Protection and Electronic Documents Act, as amended ("PIPEDA") and any similar Canadian federal or provincial legislation governing the protection of Personal Data ("Covered Canadian Personal Data").

(a) Customer will act as a controller of the Covered Canadian Personal Data and GTreasury will act as a Processor of the Covered Canadian Personal Data.

(b) Customer will provide adequate notice and obtain appropriate consents as required by, as applicable, PIPEDA and other applicable Canadian law.

(c) GTreasury shall implement security measures to protect Canada Personal Data consistent with the Underlying Agreement(s)Appendix 3 of this Addendum.

(d) Both Customer and GTreasury shall comply with all valid requests made by competent legal authorities.

(e) Upon request by Customer, GTreasury shall provide Customer with the opportunity to retrieve the Canada Personal Data.

5. **Rights in Personal Data; Right to Process**. Customer represents and warrants to GTreasury and to GTreasury's Affiliates and subprocessors that Customer has all rights (whether from consent of the Data Subjects of the Personal Data, having a legitimate interest as contemplated by GDPR Article 6, one or more derogations under GDPR Article 49, or otherwise under applicable Data Protection Law) with respect to the Covered Personal Data necessary to transfer the same to GTreasury, cause or instruct GTreasury to possess and Process such Personal Data as called for by this DPA and/or the Underlying Agreement(s), and permit GTreasury to so possess and process, and have subprocessed, such Personal Data as called for by this DPA and/or the Underlying Agreement(s). Customer will indemnify, defend, and hold harmless GTreasury and its Affiliates and subprocessors from and against any claim by or for benefit of any Data Subject, or government authority, alleging facts that, if true, would be a breach of the representations and warranties in this Section 5.

6. **EEA-Specific Provisions.** Customer, as data exporter, and GTreasury, as data importer, agree to the Standard Contractual Clauses attached as Attachment 1 as though Customer and GTreasury had executed and delivered the same. Such Standard Contractual Clauses apply solely to Covered Personal Data of Data Subjects who are in the EEA.

(a) In the case of transfers of Covered Personal Data by Customer to GTreasury, only Module Two (covering Controller-to-Processor transfers) will apply.

(b) In the case of transfers of Covered Personal Data by GTreasury to Customer, only Module Four (covering Processor-to-Controller transfers) will apply.

(c) Modules One and Three will not apply and neither Party will make any transfer to the other that is covered by either such module.

(d) For the purposes of Clause 17, the law of The Netherlands will govern the Standard Contractual Clauses.

(e) For the purposes of Clause 18, any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the The Netherlands.

7. **UK-Specific Provisions**. The following provisions apply with respect to Covered Personal Data that is covered by the UK Data Protection Act 2018 as amended (the "UK Act") (such Personal Data being "UK Covered Personal Data").

(a) Customer acts as controller and exporter of the UK Covered Personal Data and GTreasury acts as processor and importer of the UK Personal Data.

(b) "UK Addendum" means the Approved Addendum B.1.0 issued by the UK Information Commissioner's Office ("ICO") and laid before Parliament in accordance with s119A of the UK Act, as it is revised under Section 18 of those Mandatory Clauses. As of the date of the last revision of the form of this DPA, the current version of the UK Addendum is available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

(c) The Parties will comply with the terms of Part 2: Mandatory Clauses of the UK Addendum, as it is revised under Section 18 of those Mandatory Clauses;

(d) By signing this DPA, the Parties are deemed to have signed the UK Addendum;

(e) With respect to Part 1, Table 2 of the UK Addendum:

(i) Clause 7 (the Docking Clause) is excluded;

(ii) Prior authorization under Clause 9(a) (Prior Authorisation or General Authorisation) shall not apply;

(iii) The option under Clause 11 (Redress) shall not apply;

(iv) The information required by Part 1, Tables 1 and 2 of the UK Addendum is set out in Annex I to this DPA (as applicable);

(f) With respect to Table 4 Part 1 of the UK Addendum, either Party may end the UK Addendum as set out in Section 19 of the UK Addendum (but, for the avoidance of doubt, if Customer ends the UK Addendum as permitted by this Section 7(f), such ending will have no effect on Customer's obligations under any Underlying Agreement); and

(g) Any references to the "Clauses" in the Standard Contractual Clauses shall include the amendments set out in this Section 7.

8. **Transfers to Third Parties Initiated by Customer Using GTreasury Services**. For the avoidance of doubt, where the ordinary functionality of the goods, services, and/or software of GTreasury enables Customer to initiate transactions or otherwise use the goods, services, and/or software to send and/or receive information that includes Personal Data, any transfer resulting from such Customer-initiated activity is a transfer by Customer and not by GTreasury.

9. **Data Subjects as Beneficiaries.** Where, but only to the extent that, Data Protection Law requires that Customer cause GTreasury to make one or more Data Subjects of Covered Personal Data a third-party beneficiary of one or more obligations in this DPA, each such Data Subject of Covered Personal Data is an express third-party beneficiary of GTreasury's obligations under this DPA.

10. **Additional Provisions**.

(a) Services Not Covered by an Underlying Agreement. Where an obligation of GTreasury under this DPA or the Standard Contractual Clauses is not covered by the Underlying Agreement, Customer will pay GTreasury for the services associated with such obligation at GTreasury's then-current (but, in any case, commercially reasonable) rates. For example, if Customer requires administrative or similar services to meet a Data Subject demands or a data protection impact assessment and such services are not covered by the Underlying Agreement, Customer will pay GTreasury for such services.

(b) Limitation of Liability. Except as expressly provided otherwise in an Underlying Agreement and except for Customer's obligations under Section 5, the Parties' liability under this DPA will be limited to the same extent that the Underlying Agreement(s) limit(s) liability for ordinary breaches of such Agreement(s) (i.e. any exclusion from limitations of liability, or separate higher limit limitations of liability, for particular categories under an Underlying Agreement will not apply to this DPA). Nothing in this DPA limits a Party's liability to a Data Subject to the extent that applicable law prohibits such a limitation.

(c) Separate from Confidentiality Obligations. For the avoidance of doubt, the obligations under this DPA are separate and independent from any obligation of confidentiality, or limitation on use of information, (whether styled "confidentiality" or otherwise) under the Underlying Agreement(s). No exclusion from a limitation of liability for a confidentiality obligation will operate to result in unlimited liability under this DPA (including, for the avoidance of doubt, the Standard Contractual Clauses).

(d) Choice of Law. This DPA shall be governed in all respects by the governing law of the applicable Underlying Agreement.

(e) Assignment. Neither Party may assign any right or obligation under this DPA, except that either Party may assign all, but not less than all, of its rights and obligations under this DPA to any purchaser or other successor to all or substantially all of the Party's business associated with this DPA, provided only that (i) the assignee possesses financial and technical wherewithal necessary to fully perform under this DPA, (ii) the assignor gives to the other Party notice of the assignment on or before the time at which the assignment is effective, (iii) the assignment does not, by its nature, materially increase the other Party's obligations or reduce the other Party's rights, and (iv) the assignee assumes in writing all of the assignor's rights and obligations under this DPA after the effective time of the assignment. Upon any permitted assignment by a Party of its rights and obligations under this DPA, the assigning Party will have no liability for acts or omissions of the assignee after the effective time of the assignment.

(f) Notice. Any notice required or permitted to be given under this DPA must be in writing and will be deemed effective (a) if given by personal delivery, upon such personal delivery, (b) if given by nationally-recognized courier or mail service (in either case that has realtime or near-realtime tracking), at the time that the notice is delivered (or an attempt is made to deliver the notice, regardless of whether refused) to the receiver's premises according to the tracking records of the courier or mail service, or (c) if given by fax, at the beginning of the next business day at the receiver's location, provided that the sender's fax device generates a confirmation that the fax arrived at the receiver's device and that there is no indication in the course of the transmission that the notice did not arrive at the receiver's fax device. The addresses for notice for each Party are those in the preamble to this DPA. Either Party may change its address for notice by notice to the other Party.

(g) Waiver. The waiver of, or failure of either Party to exercise, any right in any respect provided for herein shall not be deemed a waiver of any further right under this DPA or a waiver of the ability to exercise the same right on a different occasion.

(h) Severability. If any provision of this DPA is invalid, unlawful, or unenforceable under any applicable statute or rule of law, the provision is, to that extent, to be deemed omitted, and the balance of the Agreement shall remain enforceable.

(i) Counterparts. This DPA may be executed in one or more counterparts.

(j) Drafting Party. No rule of law that requires that any part of the Agreement be construed against the Party drafting the language will be used in interpreting this DPA.

(k) Entire Agreement. This DPA, together with the Underlying Agreement, constitutes the entire agreement between the Parties with respect to the subject matter of this DPA and the Underlying Agreement and there are no representations, understandings or agreements about the subject matter of this DPA and the Underlying Agreement that are not fully expressed in this DPA. No amendment, change, waiver, or discharge of this DPA shall be valid unless in a record signed by the Party against whom enforcement is sought.

Signatures appear on the next page.

Signature Page to

DATA PROCESSING AGREEMENT

The Parties have each caused their authorized representatives to sign this Data Processing Agreement as of the Effective Date.

For the avoidance of doubt and as contemplated by Sections 6 and 7, by these signatures, Customer is executing the Standard Contractual Clauses and the UK Addendum as exporter/controller and GTreasury is executing the Standard Contractual Clauses and the UK Addendum as importer/processor.

GTreasury	**Customer**
By: (Signature)	By: (Signature)
(Printed name)	(Printed name)
Its: (Title)	Its: (Title)

Attachment 1

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) 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* - *E*ffect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3* - Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – 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

[Intentionally omitted.]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

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

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 without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization 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 personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

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 (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

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 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, the data 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 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. 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 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 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 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 (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.

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 with reasonable 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.

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, as communicated 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, the data 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 (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, which shall 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 with reasonable 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.

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, 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 or pseudonymisation, 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 of it 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.

(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) 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 30 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. 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 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) 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 30 days 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. 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 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. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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 data exporter.

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 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 to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

   (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

   (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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 data exporter.

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.

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 issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

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.

(b) 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.

(c) 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 to Article 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 competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

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; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

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)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

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

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(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 the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(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 data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(d) For Module Two: 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

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 Member State identified in the Data Protection Agreement to which these clauses are attached.

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 identified in the Data Protection Agreement to which these clauses are attached.

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 Member State identified in the Data Protection Agreement to which these clauses are attached.

(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 the Member State identified in the Data Protection Agreement to which these clauses are attached.

APPENDIX

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): **Customer, as identified in the Data Processing Agreement to which the Standard Contractual Clauses are attached**.

1. Name:

Customer, as identified in the Data Processing Agreement to which the Standard Contractual Clauses are attached

Address:

As identified in the Data Processing Agreement to which the Standard Contractual Clauses are attached

Contact person's name, position and contact details:

As identified in the Data Processing Agreement to which the Standard Contractual Clauses are attached

Activities relevant to the data transferred under these Clauses:

Receiving and using the goods, services, and/or software under one or more Underlying Agreements as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

Signature and date:

See signature page to the Data Processing Agreement to which the Standard Contractual Clauses are attached

By:
(Signature)

_
(Printed name)

Its: _
(Title)

Role (controller/processor):

Controller

Data importer(s): **GTreasury, as identified in the Data Processing Agreement to which the Standard Contractual Clauses are attached**

1. Name:

GTreasury, as identified in the Data Processing Agreement to which the Standard Contractual Clauses are attached

Address:

As stated in the Data Processing Agreement to which the Standard Contractual Clauses are attached

Contact person's name, position and contact details:

As stated in the Data Processing Agreement to which the Standard Contractual Clauses are attached

Activities relevant to the data transferred under these Clauses:

Performance under one or more Underlying Agreements as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

Signature and date:

See signature page to the Data Processing Agreement to which the Standard Contractual Clauses are attached

By:
(Signature)

(Printed name)

Its:
(Title)

Role (controller/processor):

Processor

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

Categories of data subjects whose personal data is transferred.

Employees, contractors, contractors, and others who receive and use GTreasury's software and/or services and/or who administer the relationship between Deque and Customer.

Persons whose personal data Customer includes in records in GTreasury's systems to the extent necessary in order for GTreasury to perform under the Underlying Agreement(s).

Categories of personal data transferred

Information customarily contained in a support ticket (e.g., name, business telephone number, business e-mail address, and organizational role).

Information necessary to provide and maintain login and similar credentials ticket (e.g., name, business telephone number, business e-mail address, and organizational role) or to bill and receive payment.

Information necessary to provide training and/or consulting services ((e.g., name, business telephone number, business e-mail address, organizational role, location, training attempted, and training received).

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

None.

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

Continuous.

Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, and/or destruction, all to the extent required to perform under the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

Purpose(s) of the data transfer and further processing

Performance under, and/or enjoyment of the benefit of, the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

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

The term of the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached, as well as any additional time that such Underlying Agreement(s) require GTreasury to retain such information and, in any case, the time, using industry-standard practices, necessary to delete such information.

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

The term of the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached, as well as any additional time that such Underlying Agreement(s) require GTreasury to retain such information and, in any case, the time, using industry-standard practices, necessary to delete such information.

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.

As described in Clause 13.

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

The technical and organisational measures required by the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

1. Name

   Microsoft Corp. (and/or such of its affiliates as provide Azure services)

   Address

   One Microsoft Way
   Redmond, Washington 98052-6399
   +1425-882-8080

   Contact person's name, position and contact details:

   Microsoft EU Data Protection Officer
   One Microsoft Place
   South County Business Park
   Leopardstown
   Dublin 18
   D18 P521
   Ireland
   Telephone: +353 (1) 706-3117

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

   Hosting services necessary to deliver the services under the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

2. Name

   Amazon Web Services, Inc. (and/or such of its affiliates as provide AWS hosting services, including, but not limited to, Amazon Web Services EMEA SARL and Amazon Internet Services Private Limited)

   Address

   410 Terry Avenue North
   Seattle, Washington 98109-5210,
   +1425-882-8080

   Contact person's name, position and contact details:

   Amazon Web Services EMEA SARL Data Protection Officer
   38 Avenue John F. Kennedy
   L-1855, Luxembourg,
   ATTN: AWS EMEA Legal

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

   Hosting services necessary to deliver the services under the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.

3. Name

   Rackspace Technology, Inc. (and/or such of its affiliates as provide hosting services)

   Address

1 Fanatical Place
Windcrest, Texas 78218
+1 210-312-4000

Contact person’s name, position and contact details:
Chief Privacy Officer
Rackspace Technology, Inc.
1 Fanatical Place
Windcrest, Texas 78218

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Hosting services necessary to deliver the services under the Underlying Agreement(s) as contemplated by the Data Processing Agreement to which the Standard Contractual Clauses are attached.