Privacy and Data Protection Agreement

January 2024

This Agreement governs whenever a Supplier or a Supplier Affiliate Processes VWTS Data or has access to a VWTS Information System in connection with the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of services and/or deliverables by Supplier to VWTS (Contract Document(s)). In the event of any inconsistency or conflict between this Agreement, Local Law and/or the Contract Document(s) with respect to a subject covered by this Agreement, the provision requiring the higher level of protection for VWTS Data shall prevail. The requirements in this Agreement are in addition to any confidentiality obligations between VWTS and the Supplier under the Contract Document(s). VWTS or the applicable VWTS Affiliate owning any of the VWTS Data being accessed pursuant to the Contract Document(s) may enforce the terms of this Agreement.

In the event Supplier or a Supplier Affiliate Processes VWTS Data that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with VWTS for VWTS's compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., Local Standard Contractual Clauses, U.S. Protected Health Information Agreement), implementation of additional security controls required by applicable law, completion of regulatory filings applicable to Supplier, and participation in regulatory audits, subject to the terms in Annex IV regarding Clause 8.9 – VWTS Audit Rights.

Supplier shall comply with all laws applicable to Supplier's activities concerning Personal Data governed by this Agreement, including those concerning notice and consent, onward transfer to a third party, and international transfer, and shall act only on VWTS's written instruction concerning any such transfers. Suppliers must receive approval from VWTS prior to (i) moving Personal Data from its VWTS-approved hosting jurisdiction to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than the hosting jurisdiction or other VWTS-approved jurisdiction.

Supplier shall inform VWTS immediately if it is no longer able to comply with this Agreement, the Contract Document(s) or other VWTS instructions.

Part A: Definitions

Part B: GDPR Standard Contractual Clauses unmodified, including Annexes I to III

Part C: Annex IV - Specific Provisions

Part D: Annex V – UK Addendum

Part E: Annex VI – Australia Addendum

Part A: Definitions

Any words following the terms "including," "include," "e.g.," "for example", "such as" or any similar expression are for illustration purposes only.

Jurisdiction specific definitions and terminology may vary slightly across global data privacy regulations. Terminology specific to Applicable Laws or Local Laws apply as part of the following definitions:

(i) Applicable Laws, or Local Laws, means the laws and policies of the Local Government and all resulting statutory and regulatory requirements applicable in the jurisdiction where the data subjects of the processing are located and where the data is processed. The definition of Applicable Laws, or

Local Laws, includes, for example, GDPR (EU), LGPD (Brazil), CCPA (California), PIPEDA (Canada), PPL (Israel), UK GDPR, Data Protection Act 2018 (UK), PDPA (Singapore), Personal Information Protection Law (China), Data Security Law (China), and Australian Privacy Laws (as defined in Annex VI).

(ii) Contact Data means the names and business contact details shared between the parties for the purpose of managing the business relationship and associated activities, such as contract management, orders, logistics, invoicing and payments.

(iii) Controller means the entity which alone or jointly with others determines the purposes and means of the processing of personal data and is responsible for decisions concerning the processing of personal data. In most cases, but not all, this would be VWTS. The definition of “Controller” includes “Business” as defined under CCPA, Database Owner as defined under PPL (Israel),Business Operator as defined under APPI (Japan) and, as applicable, "APP entity" as defined under the Privacy Act (Australia).

(iv) Controlled Data is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export controlled data. Controlled Data shall be subject to the controls below for VWTS Sensitive Data.

(v) Data Subject means the identified or identifiable individual to whom Personal Data relates. The definition of “Data Subject” includes “Consumer” as defined under CCPA and “individuals” as defined under the Privacy Act (Australia). Any data subject rights, as defined in this agreement, apply to Consumer rights.

(vi) Highly Privileged Accounts, or HPAs, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

(vii) Mobile Devices means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

(viii) Personal Data means any information that relates to an identified or identifiable natural person (Data Subject), as defined under applicable law. The definition of “Personal Data” includes “Personal Information” as defined under Applicable Laws such as California’s CCPA, the Australian Privacy Act and Japan’s APPI. Legal entities are Data Subjects where required by law.

(ix) Process(ing) means to perform any operation or set of operations upon VWTS Data, whether or not by automatic means, including but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

(x) Processor means the entity that processes personal data on behalf of the Controller. In most cases, but not all, this would be the Supplier. The definition of “Processor” includes “Service Provider” as defined under CCPA, “Holder” as defined under PPL (Israel) and, as applicable, "APP entity" under the Privacy Act (Australia).

(xi) Security Incident is any event in which VWTS Data is or is reasonably suspected to have been lost, stolen, improperly altered, improperly destroyed, used for a purpose not permitted under the Contract Document or this Appendix, subject to any unauthorized access or unauthorized disclosure, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this

Appendix. To the extent applicable, the definition of "Security Incident" includes "Eligible Data Breach" as defined under Privacy Act (Australia).

(xii) Security Notices are any written communications, notices, filings, press releases, or reports related to any Security Incident.

(xiii) Sensitive Personal Data is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance Portability and Accountability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special data categories of data under applicable data protection law (such as race, nationality, political opinions, trade union membership, religious or philosophical beliefs, genetic data, biometric data processed solely to identify a human being, home life, and sexual orientation). The definition of "Sensitive Personal Data" includes "Sensitive Information" as defined under the Privacy Act (Australia).

(xiv) Supplier is the entity that is providing goods or services to VWTS pursuant to the Contract Document.

(xv) Supplier Information System(s) means any Supplier systems and/or computers used to Process VWTS Data pursuant to the Contract Document, which includes laptops and network devices.

(xvi) Supplier Personnel means all Supplier persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates, suppliers, contractors, subcontractors and agents, as well as anyone directly or indirectly employed or retained by any of them.

(xvii) VWTS means VWTS S.A. or a VWTS S.A. affiliate signing the Contract Document with Supplier.

(xviii) VWTS Data is any VWTS Confidential Information as defined in the Contract Document Processed in connection with performance of the Contract Document. Personal Data, Sensitive Personal Data, Controlled Data and VWTS Restricted Data are VWTS Data.

(xix) VWTS Information System(s) means any systems and/or computers managed by VWTS, which includes laptops and network devices.

(xx) VWTS Restricted Data is information that VWTS identifies as 'restricted data' in the Contract Document, or that VWTS identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

Part B

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

I. The standard contractual clauses herein are the exact transcription of the Standard Contractual Clauses of the Commission Implementing Decision (EU) 2021/915 of June 4, 2021.

II. All Annexes must be completed.

III. Provisions that are non-applicable are or must be crossed out.

IV. An Annex IV has been created.

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each '**data exporter'**), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each '**data importer'**)

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to 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

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

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interprétation

(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
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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 offenses (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 ([2]) (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 benefiting 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 defense 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.

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

(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.

Clause 9
Use of sub-processors

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorization 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 ten (10) 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. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfills 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.

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

(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 fulfill 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

(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 authorized 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 organizational 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.

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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(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, organization 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

(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

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant 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 behavior 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

(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 authorizing 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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

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

(iii) any relevant contractual, technical or organizational 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 fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational 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

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

existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17
Governing law

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.]

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(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.


VEOLIA
Privacy and Data Protection Agreement
January 2024

APPENDIX

ANNEX I

A. LIST OF PARTIES

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

Name:

Click or tap here to enter text.

Address:

Click or tap here to enter text.

Contact person's name, position and contact details:

Click or tap here to enter text.

Activities relevant to the data transferred under these Clauses:

Click or tap here to enter text.

Role:

Click or tap here to enter text.

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

Name:

Click or tap here to enter text.

Address:

Click or tap here to enter text.

Contact person's name, position and contact details:

Click or tap here to enter text.

Activities relevant to the data transferred under these Clauses:

Click or tap here to enter text.

Role:

Click or tap here to enter text.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Click or tap here to enter text.

Categories of personal data transferred

Click or tap here to enter text.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Click or tap here to enter text.

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

Click or tap here to enter text.

Nature of the processing

Click or tap here to enter text.

Purpose(s) of the data transfer and further processing

Click or tap here to enter text.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

C. COMPETENT SUPERVISORY AUTHORITY

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

For European transfers, the supervisory authority in the EU Member State in which the data exporter is established. For UK transfers, the UK Information Commissioner's Office. For Australian transfers, the Office of the Australian Information and Privacy Commissioner

(**OAIC**).

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

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

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

[Examples of possible measures:

Measures of pseudonymization and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Measures for user identification and authorization

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimization

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III

LIST OF SUB-PROCESSORS

The Controller has authorized the use of the following sub-processors:

1. **Name**: Click or tap here to enter text.

   Address: Click or tap here to enter text.

   Contact person's name, position and contact details: Click or tap here to enter text.

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Click or tap here to enter text.

2. **Name**: Click or tap here to enter text.

   Address: Click or tap here to enter text.

   Contact person's name, position and contact details: Click or tap here to enter text.

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Click or tap here to enter text.

3. **Name**: Click or tap here to enter text.

   Address: Click or tap here to enter text.

   Contact person's name, position and contact details: Click or tap here to enter text.

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Click or tap here to enter text.

Part C

ANNEX IV

Specific Provisions

These specific provisions must be adhered to in addition to, or included in, the Technical and Organizational Measures documented in Annex II:

Provisions that are non-applicable or cannot be adhered to by the Supplier, are or must be crossed out.

Regarding Clause 8.1 - Instructions:

Unless and except to the extent expressly provided in the Contract Document, Supplier must seek and obtain VWTS's prior written approval regarding the scope of any Personal Data to be collected directly by Supplier.

In the case of Personal Data collected directly from Data Subjects by Supplier, Supplier shall comply with provisions regarding Clause 8.3 (below) of this Annex IV and applicable data privacy laws and regulations, including those concerning notice, consent, access and correction/deletion.

Regarding Clause 8.2 - Purpose Limitation:

Supplier and Supplier Personnel shall Process VWTS Data, and access and use VWTS Information Systems, only on a need-to-know basis and to the extent necessary to perform services under the Contract Document or as otherwise instructed by VWTS in writing.

Regarding Clause 8.3 - Transparency:

Unless and except to the extent expressly provided in the Contract Document, Supplier must seek and obtain VWTS's prior written approval regarding any notices to be provided and any consent language to be used when collecting Personal Data directly from a VWTS Data Subject.

Regarding Clause 8.5 – Duration of processing and erasure or return of data:

1. Supplier shall undertake reasonable measures to terminate Supplier Personnel's physical and logical access to VWTS Data no later than the date of separation or transfer to a role no longer requiring access to VWTS Data. Supplier shall notify VWTS of any separation or transfer of Supplier Personnel with VWTS SSO credentials no later than the day of that event.
2. Supplier shall within 30 (thirty) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of VWTS Data and return to VWTS all copies of VWTS Data. In lieu of returning copies, VWTS may, at its sole discretion, require Supplier to destroy all copies of VWTS Data, using

agreed upon methods to ensure such VWTS Data is not recoverable, and certify to such destruction.

3. Supplier may continue to retain VWTS Data beyond the period prescribed in #1 where required by law, provided that (i) Supplier notifies VWTS prior to the Contract Documents termination or expiration of the obligation, including the specific reasons for such retention; (ii) Supplier has a documented retention period and secure deletion procedure for such copies, with back-up copies retained no longer than 6 (six) months from the date on which they were captured, and legally required copies retained only to the end of their legally required retention period; (iii) following such period, all copies and back-up copies are deleted in such a manner that they are not recoverable; (iv) Supplier performs no Processing of VWTS Data other than that necessitated by retaining or deleting the relevant copies; and (v) Supplier continues to comply with all the requirements of this Agreement in relation to any such retained VWTS Data until the same is securely deleted.
4. Termination or expiration of the Contract Document, for any reason, shall not relieve the Supplier from obligations to continue to protect VWTS Data against the impermissible disclosure in accordance with the terms of the Contract Document and this Agreement.

Regarding Clause 8.6(a) – Security of processing (TOMs):

1. The processor shall refrain from making technical changes to the TOMs annexed to this Agreement that materially reduce the level of security as described in such TOMs without the prior written consent VWTS.
2. Prior to gaining access to any VWTS Data, the Supplier must be approved through the VWTS Cybersecurity risk assessment.
3. Suppliers must maintain and comply with written information security policies and procedures consistent with the requirements of this Appendix.
4. Supplier must ensure each account through which VWTS Data may be accessed is attributable to a single Supplier Personnel individual with a unique ID (not shared) and each account must require authentication (e.g., password) prior to accessing VWTS Data.
5. Where authentication mechanisms are based on passwords, suppliers must deploy multi-factor authentication in addition to strong passwords, including requirements for minimum password length, lockout, expiration period, complexity, encryption, changing of default passwords, and usage of temporary passwords. User account credentials (e.g., login ID, password) must not be shared.
6. Supplier Information Systems must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention systems (IDS/IPS) in a risk based manner, client and server-side antivirus programs

that include up-to-date antivirus definitions, and installation into production of all critical patches or security updates within thirty (30) days from the release of any such updates or patches. Suppliers must implement documented change management procedures that provide a consistent approach for controlling, implementing and documenting changes (including emergency changes) for Supplier Information Systems that includes appropriate segregation of duties.

7. Unless otherwise expressly agreed in the Contract Document, development and testing environments must be physically and/or logically separated from production environments and must not contain VWTS Data. Production changes must be approved by the Supplier's appropriate system owner and include appropriate segregation of duties.

8. Any back-up media containing VWTS Data stored at Supplier's site must be kept in a secure location with restricted physical access and be encrypted if technically feasible. If off-site media storage is used, the Supplier must have a media check-in/check-out process with locked storage for transportation.

9. An inactivity lock must be implemented on workstations when left unattended and a password or PIN must be required to enable access. Network layer security devices must allow only authorized connections, and rule sets must be reviewed.

10. Mobile Devices used to Process VWTS Data (including emails) must have centrally-managed security controls, including required passcode, minimum password length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

11. Any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing VWTS Personal Data must be encrypted at rest. Encryption also must be employed when transferring Personal Data over public networks/Internet. Suppliers must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.

Physical security controls shall include the following on all Supplier facilities where VWTS Data may be Processed:

12. Access to all Supplier locations where VWTS Data is Processed must be limited to Supplier Personnel and authorized visitors. Reception areas must be manned or have other means to control physical access.

13. Visitors at Supplier locations where VWTS Data is Processed must be required to sign a visitor's register and wear an identification badge. For data centers or similar facilities, visitors must be escorted or observed at all times.

14. Documents that contain VWTS Data must be kept secured (e.g. locked office or file cabinet) when not in use.

Regarding 8.6(b) – Security of Processing (Access by Supplier Personnel):

1. Prior to providing access to any VWTS Data to any Supplier Personnel, Supplier

must obligate them to

a. comply with the applicable requirements of the Contract Document and this Agreement. Suppliers shall take reasonable steps to ensure continuing compliance by such Supplier Personnel.
b. participate in appropriate information security awareness training and annually thereafter.

2. VWTS Data shall not be Processed on personal accounts (e.g., individual email or cloud services accounts) or on personally-owned computers, devices or media, except for personally owned devices subject to a Bring Your Own Device policy or comparable policy, through which the personal device is subject to commercially reasonable administrative, physical, and technical security measures implemented by Supplier.

Regarding Clause 8.6(c) – Security of Processing (In the event of a personal data breach):

1. Security Incidents on Suppliers Information Systems must be logged and reviewed quarterly, secured, and maintained for a minimum of twelve (12) months.

2. Suppliers must implement an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents and must perform any required recovery actions to remedy the impact.

3. Supplier shall notify VWTS without delay but no longer than within forty-eight (48) hours after discovery, or shorter if required by applicable law, of any Security Incident experienced by Supplier. Supplier shall report Security Incidents to the VWTS Contact listed in Annex I.

4. Supplier shall cooperate with VWTS as reasonably requested in its investigation of a Security Incident, at no additional cost, and complete, if necessary, the notification form sent by VWTS and send it to the VWTS Contact *and* DPO listed in Annex I. Taking into account the nature of the Processing and the information available to Supplier, any documentation or information that may be useful for VWTS to notify the competent supervisory authority and the data subjects of the data breach should be attached to the notification, if necessary, as well as the name and current contact details of the processor's DPO or any other person able to provide additional information.

5. Supplier shall collaborate with VWTS as reasonably requested, at no additional cost, to take all reasonable steps to put an end to the Security Incident, to repair as fast as possible any damage that this personal data breach may have caused, and to prevent any repetition of a similar incident.

6. The Supplier shall not communicate on or disclose the Security Incident, unless required by law. In any case, the Supplier shall not include VWTS in its communication without VWTS's prior written approval. Should VWTS elect to send a Security Notice regarding a Security Incident, Supplier shall provide reasonable

and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.

7. Other than approved Security Notices, or to law enforcement or as otherwise required by law, Supplier may not make or permit any public statements concerning VWTS's involvement with a Security Incident to any third-party without explicit written authorization of VWTS's Legal Department.

Regarding Clause 8.7 – Sensitive Data:

These Clause 8.7 provisions 1-12 apply to Suppliers that Process Sensitive Personal Data, Controlled Data, and/or VWTS Restricted Data. The requirements of these Clause 8.7 provisions are in addition to all other requirements contained in this Agreement. References to VWTS Sensitive Data in these Clause 8.7 provisions shall be deemed to also refer to VWTS Restricted and/or Controlled Data as the context requires.

1. Suppliers must have a formal information security program with clearly defined information security roles, responsibilities, and accountability.

2. Suppliers must perform or have an independent third party perform vulnerability assessments on Supplier Information Systems annually and remediate as required in the section below, regarding clause 8.9(c) - Supplier Audit Responsibilities.

3. Any Supplier Personnel accessing Supplier's internal or hosted network remotely must be authenticated using two-factor authentication method and such transmissions must be encrypted at a level consistent with industry standards.

4. Suppliers must implement a device hardening and configuration standard.

5. Suppliers must implement appropriate data loss prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of VWTS Restricted Data from Supplier Information Systems.

6. Suppliers must implement processes to support the secure creation, modification, and deletion of HPAs. Suppliers must review and update HPA access rights quarterly. HPA usage must be reviewed weekly. All HPA access must be established using encrypted mechanisms (e.g., secure shell).

7. Suppliers must dispose of paper records containing VWTS Sensitive Data, and remove VWTS Sensitive Data from Supplier Information Systems, in an auditable manner that ensures that the VWTS Sensitive Data may not be accessed or readable.

8. Encryption must be implemented in the following instances: (i) any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing VWTS Sensitive Data must be encrypted at rest; (ii) where technically feasible, VWTS Sensitive Data must be stored in encrypted form, except

where encryption is mandatory in such cases as set forth above; and/or (iii) transferring VWTS Sensitive Data over public networks (such as the Internet).

9. Where encryption is required, Suppliers must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.

10. Supplier Information Systems consisting of servers and/or network equipment used to store or access VWTS Restricted Data must be kept in a secure room with enhanced logical and physical access control, and located on the interior of the building with no windows unless safeguards are in place to prevent shattering and unauthorized entry.

11. Physical access must be monitored, recorded and controlled with physical access rights reviewed annually. Physical access logs detailing access must be stored for six (6) months unless prohibited by local law. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained for at least thirty (30) days.

12. Suppliers must receive approval from VWTS prior to moving VWTS Sensitive Data from its VWTS-approved physical location or jurisdiction to a different physical location or jurisdiction.

These Clause 8.7 provisions # 13-16, regarding Disaster Recovery, apply to any Supplier Information System(s) that (i) Processes VWTS Restricted Data, Controlled Data, and/or Sensitive Personal Data, and/or (ii) where an outage of the Supplier Information System(s), as identified in the Contract Document and/or this Agreement, is likely to significantly adversely impact VWTS or overall VWTS operations, financial position, regulatory compliance, and/or reputation.

Unless a disaster recovery (DR) program is otherwise set forth in more detail elsewhere in the Contract Document, Supplier must maintain a DR program for all Supplier Information Systems and facilities used to provide services under the Contract Document to VWTS. The DR program must be designed to ensure that the Supplier has a methodology by which a system can continue to function through an operational interruption or disaster. The DR program shall include the following elements:

13. Supplier's operational procedures must verify the successful completion of backups and the backup media must be tested regularly (at minimum semi-annually) to ensure it will operate in the event of an emergency.

14. For rooms containing Supplier Information Systems consisting of servers and/or network equipment used to provide services to VWTS, controls must be implemented to mitigate the risk of power failures, and environmental conditions.

15. DR plans must be implemented for all Supplier Information Systems and facilities that are used to provide services to VWTS.

16. Suppliers must conduct full scale DR tests annually for Supplier Information Systems that are used to provide services to VWTS to ensure that such Supplier Information Systems can be recovered in a manner that meets the contractual service levels specified in the Contract Document. DR results must be documented and provided to VWTS upon request.

Regarding Clause 8.8 – Onward Transfers, 10(a) – Notification of Data Subject Request(s) and 15.1 – Notification in case of access by public authorities:

Unless prohibited by law, Supplier shall notify VWTS promptly and act only upon VWTS's instruction concerning any request by a third party, including public authorities, for disclosure of VWTS Data or for information concerning Supplier's Processing of VWTS Data, as well as any request received from an individual concerning his/her Personal Data.

Regarding Clause 8.9 (c) – Documentation and Compliance (ability to demonstrate):

In this respect, the Supplier shall in particular provide, at the request of VWTS, extracts from their own register relating to the processing activities carried out on behalf of VWTS in order to enable them to keep their own register up-to-date. The register shall include a current inventory of all hardware and software used to process VWTS Data.

SUPPLIER AUDIT RESPONSIBILITIES:

1. Suppliers must conduct periodic security risk assessments of Supplier Information Systems to identify critical information assets, assess threats, and determine potential vulnerabilities.

2. Upon request, Supplier must provide VWTS either A) its (1) ISO 27001 certificate and (2) SSAE 16 Type 2 audit reports, or B) an executive summary of any audits and assessments conducted on Supplier Information Systems. Either option must include the scope of the audit and/or assessment and any vulnerabilities and corrective actions.

3. Suppliers must use commercially reasonable efforts to remediate within thirty (30) days any items rated as high or critical (or similar rating) in any audits or assessments of Supplier Information Systems.

4. Supplier agrees to cooperate fully with VWTS or its designee during audits (below) and shall provide access to facilities, appropriate resources, and supporting documentation and complete security assessment questionnaires as requested.

VWTS AUDIT RIGHTS:

5. VWTS reserves the right to conduct an audit, upon 30 days advance notice, of Supplier's compliance with the requirements in this Agreement, including but not limited to: (i) review of Supplier's applicable policies, processes, and procedures, (ii) review of the results of Supplier's most recent vulnerability assessment and accompanying remediation plans, and (iii) on-site assessments during regular

business hours of Supplier's physical security arrangements and of the portion of Supplier Information Systems that are dedicated to providing Services to VWTS (but not Supplier Information Systems that process data of other Supplier customers). VWTS reserves the right to conduct an Applications Vulnerability Assessment if Supplier's vulnerability assessments do not meet or exceed VWTS application security requirements. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes VWTS Data.

6. If the audit reveals that the security measures implemented by Supplier and/or its sub-processor are not sufficient or appropriate, or if these measures reveal the existence of breaches or do not comply with the terms of this Agreement and/or laws applicable to Supplier's activities under the Agreement, Supplier shall, at its own expense, implement corrective measures within a period agreed between the Parties, taking into account the nature and seriousness of the breach, without prejudice to the data controller's other rights, in particular the rights to obtain compensation and/or to terminate the Contract.

7. The Parties agree that the audit procedure shall not exempt the processor from compliance with its contractual obligations regarding the protection of personal data.

Regarding Clause 9 – Use of sub-processors:

Supplier acknowledges and agrees that no data transfer will occur and/or that such transfer will be suspended immediately if the sub-processor is not or is no longer able to comply with Clause 9 of the SCCs.

Regarding Clause 10 – Data subject rights:

Clause 10(a) of these Clauses provides that the processor shall promptly notify the controller of any data subject request. In this respect, the Supplier hereby undertakes to notify VWTS within 5 days following the receipt of any such request(s).

Clause 10(b) of these Clauses provides that the processor shall assist the controller in fulfilling its obligations to respond to concerned data subjects' requests to exercise their rights.
In this respect, taking into account the nature of the Processing and the information available to the Supplier, the Supplier hereby undertakes to do the following at no additional cost:

- Provide VWTS, without undue delay and, to the extent possible, within 5 days following the VWTS request, with documents and information requested by VWTS relating to the data processing;

- Carry out, without undue delay and, to the extent possible within 5 days, any instruction from VWTS relating to the communication, rectification and deletion of data, or limitation or termination of the processing. Upon VWTS's request, the Supplier shall demonstrate, by any means, that it has duly carried out the VWTS instructions in accordance with this provision.

Regarding Clause 15.1 – Notification Obligations of the data importer in case of access by public authorities:

The Supplier shall inform VWTS as soon as possible of any request (including any investigation or search) from a competent authority which it directly received, and which relates to the processing of VWTS personal data implemented under these Clauses. In the event that VWTS is the subject of an investigation by a data protection authority or any other competent authority, of proceedings arising from a criminal or administrative offense, of a liability claim by a concerned data subject or third party, or of any other claim or legal action relating to the processing of personal data implemented under the standard clauses, the Supplier undertakes to take all reasonable steps to assist the controller at no additional cost.

Miscellaneous:

Privacy Impact Assessment

In the event that a data protection impact assessment must be made, the Supplier shall provide VWTS with all the information in its possession required to carry out said assessment as requested by VWTS and shall immediately inform VWTS in writing of any changes or modification that may impact the processing and/or the assessment. The Supplier undertakes to put in place, within the time limit set in consultation with VWTS, any reasonable measures that may become necessary as a result of the data protection impact assessment, designed to reduce the risks associated with the data it processes on behalf of VWTS to an acceptable level.

Contact

The contact person within each party for any request/question/notification in connection with these Clauses shall be the person whose contact information is set forth in Annex I above and shall be provided by the processor to any sub-processor duly authorized in accordance with the standard clauses.

Contact Data

Where one of the Parties and/or its affiliated entities processes the personal data of the employees and representatives of the other Party and/or affiliated entity, including their names and business contact details (hereinafter the "Contact Data"), for the purpose of managing their business activities (in particular, the management of the file of suppliers, customers or prospects, contract management), this Party will act in its capacity as data controller and will have to comply with the obligations incumbent on it by virtue of the applicable data protection regulations.

The data controller will retain the Contact Data of the processor for as long as necessary to fulfill the purposes for which it is to be used, subject to the legal provisions on archiving and retention periods, if any. The Contact Data will be retained according to the relevant party's Retention Policies in order to allow the data controller to demonstrate compliance with its legal and/or contractual obligations, if any, and to

ensure the follow-up of the business relationship with the provider.

The data controller and/or each affiliated entity may also be required to provide access to the Contact Data to its affiliated entities and partners who need it in the context of the services and/or for the purpose of monitoring the commercial relationship.

Where the Supplier processes Contact Data of employees and representatives of VWTS and/or the affiliated entity for the purpose of managing their customers and prospects, the Supplier will act as the data controller and undertake to comply with its obligations under the applicable data protection regulations.

To the extent permitted by Applicable Laws, such processing will be based on the legitimate interest of the Parties and/or the affiliated entity.

The Supplier shall inform its employees and representatives of the processing of their Contact Data under the conditions described in this clause, including how to exercise their rights with VWTS. Solely where permitted by Applicable Laws, the Supplier's employees and representatives have the right to access, rectify or delete such Contact Data, the right to limit the processing of such Contact Data, the right to object to the processing of such Contact Data. They may assert these rights directly by email to the VWTS DPO.

Part D

ANNEX V

UK Addendum

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

Part 1: Tables

Table 1: Parties

Start date	As set forth in Annex I.A of the Approved EU SCCs	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set forth in Annex I.A. of the Approved EU SCCs (on behalf of its UK Affiliate(s))	As set forth in Annex I.A. of the Approved EU SCCs
Key contact	As set forth in Annex I.A. of the Approved EU SCCs	As set forth in Annex I.A. of the Approved EU SCCs
Signature (if required for the purposes of section 2)	As set forth in Annex I.A. of the Approved EU SCCs	As set forth in Annex I.A. of the Approved EU SCCs

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		☐ **Option 1**: The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: ☒ **Option 2**: Or the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	**Module in Operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter**
2	✓	✓	**N/A**	☐ **Prior authorisation** ☒**General authorisation**	**10 business days**	-

Table 3 – Appendix Information

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

Annex 1A: List of Parties: See Table 1 above.

Annex 1B: Description of Transfer: As set forth in Annex I.B of the Approved EU SCCs.

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: As set forth in Annex II of the Approved EU SCCs.

Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Annex III of the Approved EU SCCs.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19 of the Mandatory Clauses (referenced below): X Importer X Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Part E

ANNEX VI

Australia Addendum

This addendum sets out the terms and conditions on which Veolia Water Technologies & Solutions Australia Pty Ltd (ACN 84 001 221 941) (**VWTS Australia**), as the applicable VWTS SA Affiliate signing the Contract Document with the Supplier, permits the Supplier (its sub-processor(s) and/or each member of Supplier Personnel) to process VWTS Data or to access a VWTS Australia Information System in connection with the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of services and/or goods under the Contract Document by Supplier to VWTS Australia.

The parties each acknowledge and agree that the obligations set out in Parts A –D of this Agreement will be subject to the terms set out in this Annex VI which, (together with the relevant provisions in Parts A- D), govern the exporting of Personal Information by the data exporter to a data importer insofar as the transfer originates from Australia or relates to Personal Information of an individual located in Australia (**Australian Personal Information**).

1. Definitions

The following definitions will be inserted, or, if there are corresponding provisions, replace those corresponding provisions in Part A of this Agreement. Terms not defined in this Annex VI have the meaning given to them in Part A. **Australian Privacy Laws** means all Australian (including Federal, State and/or Territory) privacy legislation governing the collection, holding, use, disclosure, processing and all similar handling of Personal Information, including the *Privacy Act 1988 (Cth)* (**Privacy Act**), the Australian Privacy Principles (**APPs**), the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (**NDB Scheme**), the SPAM Act, 2003, *Do Not Call Register Act* and all related and ancillary codes of conduct, guidelines and statutory regulations that apply to the handling of Personal Information in Australia, as each may be amended, superseded or replaced from time to time;

Competent Supervisory Authority means the Office of the Australian Information and Privacy Commissioner or **OAIC**;

Eligible Data Breach has the meaning given to it by the NDB Scheme under Australian Privacy Laws being any actual or suspected:

a. unauthorized access to or unauthorized disclosure of Personal Information, or a loss of Personal Information, that an organization holds;

b. that is likely to result in serious harm to one or more individuals, and

c. the organization has not been able to prevent the likely risk of serious harm with remedial action;

Personal Data means Personal Information;

Personal Information has the meaning given under the Australian Privacy Act being any information or opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not;

Sensitive Data means Sensitive Information; and **Sensitive Information** has the meaning under the Australian Privacy Act being Personal Information that includes information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record, health information, genetic information (that is not otherwise health information of an individual) and certain aspects of biometric information that is to be used for the purposes of automated biometric verification or identification or biometric templates, as each are more particularly set out in the Privacy Act.

2. Specific Obligations

2.1 Applicable Data Protection Laws

(a) The parties agree that the applicable data protection laws for the handling and transfer of Australian Personal Information are the laws applicable to the data exporter.

(b) Without prejudice to the application of Local Laws, the Supplier will comply (and will procure that each member of Supplier Personnel and each sub-processor comply(ies)) with Australian Privacy Laws (including the APPs) and any reasonable directions and requirements of VWTS Australia in relation to the collection, use, disclosure, handling, destruction, de-identification and other processing of Australian Personal Information.

(c) The Supplier warrants to VWTS Australia that it has taken such steps as are reasonable in the circumstances to ensure that it, and any of its sub-processor(s) acting as the data importer, comply with the Australian Privacy Laws and will not breach Australian Privacy Laws in relation to the handling of Australian Personal Information.

2.2 Processing of VWTS Data

(a) Without limiting the Supplier's obligations under Clause 2.1 above, Supplier will process and handle VWTS Data, including Australian Personal Information, on a need-to-know only basis and solely to the extent necessary to perform services under the Contract Document, in accordance with:

(i) Australian Privacy Laws,

(ii) VWTS Australia's lawful instructions, and

(iii) the provisions of this Annex VI,

(and in the event of any conflict in respect of the relevant standard, the highest standard will prevail).

(b) In particular, the Supplier must:

(i) not collect, use or disclose Australian Personal Information unless the information is reasonably necessary for one or more of the Supplier's declared functions or activities; and

(ii) take such steps as are reasonable in the circumstances to ensure that Australian Personal Information which it:

(A) collects is accurate, up-to-date and complete; and/or

(B) uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant;

(c) not process or handle Australian Personal Information for the purposes of any direct marketing (or of facilitating direct marketing) at any time without the prior written consent of VWTS Australia;

(d) not adopt, use or disclose any 'government related identifier' (as that term is defined under the Australian Privacy Act) forming part of Australian Personal Information unless under a specific direction of VWTS Australia and the adoption, use or disclosure is in accordance with Australian Privacy Laws.

2.3 If the Supplier no longer needs Australian Personal Information for any purpose for which the Australian Personal Information may be used or disclosed by Supplier in accordance with this Annex VI, the Contract Document or any further agreement between the parties, Supplier must (and must procure that each member of Supplier Personnel and each sub-processor) take such steps as are reasonable in the circumstances to, (at VWTS Australia's option and direction), return or destroy the Australian Personal Information or to ensure that the Australian Personal Information is de-identified to the satisfaction of VWTS Australia.

2.4 Sub-processing and onwards transfers

(a) Supplier may only engage the sub-processor(s) expressly authorized by VWTS Australia at the date of this Agreement, as listed in Appendix 3 to this Annex VI, for the processing of VWTS Data.

(b) Where Supplier proposes to engage any new sub-processor for the processing of VWTS Data following the date of this Agreement, Supplier will:

(i) notify VWTS Australia in writing of Supplier's intention to use the new sub-processor at least ten (10) working days in advance of any appointment, giving VWTS Australia sufficient time to be able to object to such changes prior to the Supplier's engagement of any sub-processor;

(ii) provide VWTS Australia with all information necessary to enable VWTS Australia to exercise its right to object.

(c) In all cases where the Supplier proposes to engage any sub-processor to handle or process Australian Personal Information, the Supplier must:

(i) enter into a written agreement with the proposed sub-processor which includes the terms, including data privacy and security measures no less protective of VWTS Data (including Australian Personal Information), than those set out in this Annex VI, including but not limited to, an obligation to comply at all times with Australian Privacy Laws in the collection, use, disclosure, destruction, de-identification or other handling and processing of Australian Personal Information and to comply with the technical and organizational security measures set out in Appendix 2 to this Annex VI; and

(ii) remain fully liable for any breach of this Annex VI or of Australian Privacy Laws that is caused by, arises out of or in connection with, any act, error or omission of a sub-processor to the extent that Supplier would have been liable had it been caused by, arose out of or in connection with the act, error or omission of the Supplier.

2.5 Technical and organizational measures

(a) Supplier agrees to take all reasonable steps to put in place security measures to protect VWTS Data against misuse, interference, accidental or unlawful destruction or accidental loss, modification, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

(b) Without limiting the foregoing, the Supplier will (and will procure its sub-processors will) implement and maintain compliance with the technical and organizational measures set out in Appendix 2 to this Annex VI and to review the appropriateness of such measures on an ongoing basis in light of the processing activities, taking into account the frequency of transfer and sensitivity of VWTS Data, including Australian Personal Information.Such security measures may include the preparation and implementation of a data breach policy and response plan that includes a process for notifying the OAIC and any affected individuals, in the event of an Eligible Data Breach.

(c) Suppliers shall refrain from making technical changes to the technical and organizational measures set out in Appendix 2 to this Annex VI that materially reduce the level of security as described in such technical and organizational measures without the prior written consent of VWTS Australia.

2.6 Security Incidents and Eligible Data Breaches

(a) If a Security Incident relates to Australian Personal Information, in addition to any other obligations set out in this Agreement, Supplier must immediately notify VWTS Australia in writing as soon as it becomes aware that there:

(i) has been an Eligible Data Breach; or

(ii) are reasonable grounds to suspect that there may have been an Eligible Data Breach

arising out of, in connection with or relating to Australian Personal Information.

(b) Without limiting any obligations under Part C of this Agreement, Supplier will (and will procure each member of Supplier Personnel and each sub-processor will)

(i) cooperate (at no additional cost) with VWTS Australia as reasonably requested in its investigation of a Security Incident. Without limitation, Supplier must supply any documentation and/or information and provide such assistance as may be requested or required by VWTS Australia or any of its affiliates so that VWTS Australia can comply with the statutory obligations applicable to it under Australian Privacy Laws, including the obligation to notify the OAIC and, as required, individuals affected by any Security Incident that involves an Eligible Data Breach; and

(ii) take all such remedial actions and measures as authorized and approved in writing in advance by VWTS Australia to prevent the likely risk of any *serious harm* to one or more individuals, as such italicized terms are defined under the Australian Privacy Act.

2.7 Co-operation and Assistance

(a) Supplier will:

(i) co-operate, and assist VWTS Australia, on request in co-operating with, and responding to applicable Australian regulators, including the OAIC and/or Australian law enforcement authorities where requests, enquiries or orders (together with relevant justifications) are being made with regard to VWTS Data, including Australian Personal Information;

(ii) unless legally prohibited from doing so, in which event, Supplier will provide details in writing to VWTS Australia of the basis and scope of this legal prohibition:

(A) make available, upon request from any of: (i) VWTS Australia; (ii) an applicable Australian regulator, including the OAIC; and/or (iii) Australian law enforcement authorities all files, documents and information required for the purposes of any review or audit of the Supplier's (or any subprocessor(s)') data processing, storage, transfer and/or handling activities relating to Australian Personal Information; and

(B) inform VWTS Australia immediately if it receives any legally binding request for disclosure of Australian Personal Information by the OAIC, any other supervisory regulator or authority or any law enforcement authority in Australia or otherwise.

(b) The Supplier acknowledges and agrees that (unless otherwise directed in writing by VTWS Australia) VWTS Australia, as employer, must respond directly to any request(s) for access or correction made by an individual with regard to their Australian Personal Information. Accordingly, Supplier will (and will procure that each member of Supplier Personnel and each sub-processor(s)):

(i) promptly inform and notify VWTS Australia of any request(s) that it (or any member of Supplier Personnel or any sub-processor) has received directly from any individual;

(ii) assist and cooperate with VWTS Australia to enable VWTS Australia to respond to any such individual request; and

(iii) not otherwise respond to any such individual request without the prior written consent of VWTS Australia

3. General

3.1 Jurisdiction

(a) Insofar as any action or dispute (including any non-contractual dispute) relates to Australian Personal Information, this Annex VI will be governed by and constructed in accordance with the laws of New South Wales, Australia and the Commonwealth of Australia.

(b) Any legal action in relation to Australian Personal Information under this Annex VI brought against any party must be brought in any court of competent jurisdiction in the State of New South Wales, Australia and each party submits to the non-exclusive jurisdiction of the courts of New South Wales, Australia.

Appendix 1: Transfer Details

A. LIST OF PARTIES

Data Exporter(s):

Name:

Click or tap here to enter text.

Address:

Click or tap here to enter text.

Contact person's name, position and contact details:

Click or tap here to enter text.

Activities relevant to VWTS Data transferred under this Annex VI:

Click or tap here to enter text.

Role:

Click or tap here to enter text.

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

Name:

Click or tap here to enter text.

Address:

Contact person's name, position and contact details:

Click or tap here to enter text.

Activities relevant to VWTS Data transferred under this Annex VI:

Click or tap here to enter text.

Role:

B. DESCRIPTION OF TRANSFER

Categories of individuals whose Personal Information is transferred

Click or tap here to enter text.

Categories of Personal Information transferred

Click or tap here to enter text.

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

Click or tap here to enter text.

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

Nature of the processing

Purpose(s) of the data transfer and further processing

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

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

Click or tap here to enter text.

C.COMPETENT SUPERVISORY AUTHORITY

Office of the Australian Information and Privacy Commissioner

GPO Box 5288

Sydney NSW 2001, Australia

Appendix 2: Technical and Organizational Measures

[Insert description of the technical and organizational measures implemented by the Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons]

Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Measures for user identification and authorization

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimization

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For onwards transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the Data Exporter

Appendix 3: List of Sub-processors

VWTS Australia has authorized the use of the following sub-processor(s):

1. **Name**:

   Address:

   Contact person's name, position and contact details:

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

2. **Name**:

   Address:

   Contact person's name, position and contact details:

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

3. **Name**:

   Address: Click or tap here to enter text.

   Contact person's name, position and contact details:

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