FirstRand

FIRSTRAND GROUP DATA PROTECTION POLICY FOR SUPPLIERS AND BUSINESS PARTNERS

November 2022

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE

FirstRand Limited and its subsidiary companies, including divisions, segments and business units (referred to as **FirstRand** or **the group**) recognise that personal information (**PI**) and records are important assets that must be protected. This document establishes a governance framework that sets out ethical and sound PI protection practices that are to be followed by all suppliers and business partners appointed by the group. This policy sets out the minimum PI protection requirements applicable to suppliers and business partners to preserve the integrity, confidentiality and availability of PI or records furnished to suppliers and business partners during the course and scope of their engagement with the group.

This policy will set out the rules of engagement in relation to how PI is handled by suppliers and business partners on behalf of FirstRand, as well as the minimum legal requirements that FirstRand requires suppliers and business partners to adhere to, including compliance with the requirements of the Protection of Personal Information Act 4 of 2013 (**POPIA**), the General Data Privacy Regulation (**GDPR**) and other legislation, where applicable from time to time, in their capacity as service providers or business partners to the group. This policy is applicable to all suppliers and applicable business partners who engage with the group and handle PI as defined in applicable law.

All group suppliers and business partners are expected to comply with all local legislative requirements within the jurisdiction in which they operate.

This policy serves as an additional measure which specifies the requirements that FirstRand has in relation to how suppliers and business partners are required to organise themselves and provide goods and/or services or collaborate in relation to agreements concluded with FirstRand and its affiliates.

FirstRand subscribes to the higher of the host-or-home principle when dealing with jurisdictions outside of South Africa. This means that where the supplier or business partner conducts business activities within a jurisdiction where the PI protection laws and regulations are of a higher standard than POPIA, then the provisions of those laws and regulations will take precedence over the provisions of POPIA, and vice versa.

2 DEFINITIONS

The following concepts will be used throughout this policy and are defined as follows:

Affiliate	Means (a) any subsidiary or a holding company or a subsidiary of the holding company of either party, or (b) any entity that controls, is controlled by or is under common control with either party. The terms "subsidiary" and "holding company" will have the meaning assigned thereto in Chapter 1 of the Companies Act, No. 71 of 2008 (the Companies Act). The term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity through the ownership of voting securities representing 50% (fifty per cent) plus 1 (one) of the possible votes.
Agreement	Means the agreement entered into between the group and the supplier or business partner, as applicable.
Associate	Shall mean any entity or unincorporated joint venture in which FirstRand has the right to receive at least 20% (twenty per cent) of the profit share or similar benefit derived from such entity or unincorporated joint venture.

Business partner	A business partner, in the context of this policy, means a natural or juristic person (**person**) holding a business relationship with the group, where such relationship does not fall within the category of a supplier, employee or customer relationship, and which person processes PI for, on behalf of or together with FirstRand under the terms of the applicable agreement between the group and the person. (*For the avoidance of doubt, the term **business partner** is used for the sake of convenience and for descriptive purposes only and should not be construed to imply a partnership between the group and the business partner in a legal sense or as understood in law.)*
Child	A child is a natural person who is defined as a child by a country's legislation and who has not been recognised as an adult by the courts of a country.
Competent person	Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of PI.
Customer	A customer is a natural or legal person who is a group customer or a person who provided their PI/SPI to the group in the context of a sale of acquiring goods or services.
Data subject	Means the person to whom PI relates. In reference to the group, this primarily but without limitation means customers, employees and operators/suppliers, other persons and third parties.
Employee	Means a person employed for wages or a salary, including permanent employees, non-permanent employees, contractors, secondees and contingent workers.
FirstRand or the group	Means FirstRand Limited and its subsidiary companies, including divisions, segments, and business units. Certain subsidiary companies may be excluded from the group description for the purposes of this policy (such as where the group is involved in private equity investments). Confirmation as to whether this policy applies to a specific company (a registered legal entity) associated with the group can be sought through the contact details provided in this policy. In this policy, any reference to "the group" or "FirstRand" includes any one or more (if they are acting jointly) group companies and all affiliates, associates, cessionaries, delegates, successors in title or third parties (authorised agents and contractors), when such parties are acting as responsible parties, joint responsible parties or operators in terms of applicable privacy laws, unless stated otherwise.
Generative artificial intelligence (GAI)	Generative artificial intelligence refers to a category of artificial intelligence technology that generates new outputs based on the data it has been trained on. Unlike traditional artificial intelligence systems that are designed to recognise patterns and make predictions, generative artificial intelligence creates new content in the form of images, text, audio, and more.
Juristic person	Means an existing company, corporation, trust, not-for-profit organisation or other legal entity recognised by law as having rights and duties.
Legislation	Means relevant and applicable data privacy and protection legislation, including but not limited to: • the Protection of Personal Information Act 4 of 2013 (POPIA); • the General Data Protection Regulation (GDPR); • the Data Protection (Bailiwick of Guernsey) Law, 2017; • the Data Protection (Jersey) Law 2018; and • the UK's Data Protection Act 2018.
Natural person	Means an identifiable, living human being.

Operator	Means a person who processes PI for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. This means any party that processes information on behalf of FirstRand.
PAIA	The Promotion of Access to Information Act 2 of 2000.
PCI standard	Means Payment Card Industry standard.
Personal information (PI)	Means information relating to an identifiable, living, natural person and where it is applicable an identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other PI relating to the person or if the disclosure of the name itself would reveal information about the person. In reference to this policy, PI must be seen primarily but without limitation as PI of group customers, employees and suppliers, and other persons and third parties.
PIN	Means "personal identification number", which is a secret numeric password known only to the user and a system to authenticate the user to the system.
POPIA	Protection of Personal Information Act 4 of 2013.
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning PI, including: (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Public record	Means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Record	Means any recorded information: (a) regardless of form or medium, including any of the following: (i) writing on any type of material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) a label, marking or other writing that identifies or describes anything of which it forms a part, or to which it is attached by any means; (iv) a book, map, plan, graph or drawing;

	(v) a photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) being in the possession of or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Responsible party/ies	Means a public or private body or any other person which/who, alone or in conjunction with others, determines the purpose of and means for processing PI. In reference to this policy, the responsible parties are the FirstRand entities as defined above.
Sensitive cardholder PI	This information includes but is not limited to card validation codes/values, full track PI (from the magnetic strip or equivalent on a chip), PINs and PIN blocks. Authentication must be against cardholders and/or authorised payment card transactions in terms of PCI.
Special personal information (SPI)	Means any PI of a data subject, concerning: (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to: (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Supplier	Means a natural or juristic person who provides a product or renders services to the group.
DEFINITIONS FROM THE GDPR	
Controller	Means a juristic person in the group, registered in the United Kingdom, Guernsey or Jersey who, alone or jointly with others, determines the purposes and means for processing PI. Such purposes and means will be determined by the GDPR or privacy laws in the United Kingdom, Guernsey or Jersey.
Processor	Means a juristic person who processes PI on behalf of the controller.
Sub-processor	Means a juristic person defined in Annexures A1, A2 and A3 of this policy.

3 APPLICABILITY

This policy is applicable to all suppliers and business partners who collect and/or process PI and or/records for, on behalf of or together with the group. The group will at the time of the conclusion of any agreement, and regularly during the course and scope of its agreement with suppliers or business partners who collaborate with the group or provide goods and/or services which require the collection and/or processing of PI and/or records in accordance with this policy, provide them with a copy of this policy.

4 SCOPE OF APPLICATION

This policy is applicable to all PI, SPI and children's PI collected, retained, processed and disseminated by all suppliers and applicable business partners for, on behalf of, or together with the group in terms of an agreement between the group and the supplier or the business partner. This includes but is not limited to PI, SPI and/or children's PI of the employees of the group, group customers, employees of group customers, and third parties whose PI is in the possession of the group and subsequently processed on the group's behalf by the supplier or business partner.

This policy supports FirstRand's internal policies. Suppliers and business partners will be informed if they need to adhere to any other internal policy.

5 SUPPLIERS AND BUSINESS PARTNER OBLIGATIONS WHEN DEALING WITH PI AND RECORDS

5.1 Accountability

5.1.1 The supplier or business partner acknowledges and accepts that any PI and/or records received from the group and/or created by it for or on behalf of the group will not become the property of the supplier or business partner.

5.1.2 The supplier or business partner shall at all times be solely and fully responsible for all its employees, agents, subcontractors and other third parties who act on its behalf in the performance of their functions in terms of its relationship with the group.

5.1.3 The supplier or business partner may only make use of agents, subcontractors and third parties for the processing of the PI if:

- the group has been informed of the agent, subcontractor and third party used and such agent, subcontractor and third party has been approved by the group in writing;
- the supplier or business partner has conducted a privacy risk assessment of the agent, subcontractor and third party and the said agent, subcontractor and third party has passed the risk assessment and has the appropriate and necessary controls to mitigate any privacy risks; and
- the supplier or business partner concludes agreements with such agents, subcontractors and third parties on no less onerous terms than that which the supplier or business partner agreed on with the group.

5.1.4 By contracting with the group the supplier or business partner, in its performance of its mandate or the obligations under the applicable agreement, undertakes that its employees, agents, subcontractors and other third parties who act on its behalf in the performance of its functions in terms of its relationship with the group, and who shall have access to the group's PI and/or records, have signed the appropriate confidentiality undertakings; and that the supplier or business partner acknowledges and confirms that:

- it has appropriate internal policies dealing with privacy and security in place for purposes of compliance with privacy legislation;
- it has external privacy notices or policies which advise data subjects how it processes PI and which notices are aligned to the disclosure obligations of privacy legislation;
- its employees, agents, subcontractors and third parties have been provided with the appropriate training to ensure that they understand the provisions of privacy legislation and PI privacy principles in general, as well as their roles and responsibilities in relation to the provision of service to the group as a responsible party;
- it will at all times adhere to the provisions, updates and amendments of privacy legislation;
- when processing PI of children or SPI, it will at all times act in accordance with any special provisions provided for in privacy legislation and the provisions of the agreement with the group; and
- it will share PI with its agents, employees' subcontractors and other third parties only as strictly necessary, and to the extent necessary to process the PI in accordance with the agreement with the group.

5.1.5 During the course and scope of its agreement with the group, the supplier and/or business partner will not utilise group PI, SPI and/or records, including proprietary information, on GAI technologies in the provision of their services to the group. If the supplier and/or business partner is dependent on these technologies to provide a service to the group, the supplier and/or business partner must obtain prior written authorisation from FirstRand to do so. Where the supplier and/or business partner obtains approval to utilise GAI platforms, it shall be prohibited from utilising GAI in a manner that is inappropriate and contrary to the group's policies and standards. The supplier and/or business partner shall also refrain from the following activities (the below list is not exhaustive):

- utilising group PI, SPI and/or records, including proprietary information, in natural language processing or predictive analytics on an open-source GAI platform;
- utilising GAI that exploits the vulnerabilities of a specific group of persons due to age or any SPI categories which will lead to detrimental or unfavourable treatment of data subjects; and
- utilising GAI in a manner that contravenes data privacy and protection laws and copyright infringement laws.

The following policy statements relate only to the GDPR, the UK Data Protection Act 2018 and the UK GDPR, where in scope:

5.1.6 Where the supplier or business partner is confirmed as a processor by the group, and where, as a result of providing the service to a controller and such a service requires the collection and/or processing of PI belonging to the controller, the controller and the supplier will conclude a PI transfer agreement on the terms outlined in Annexures A1, A2 and A3 (which are not negotiable).

5.1.7 Where the supplier or business partner is confirmed as a sub-processor by the group, as a result of providing the service to the group, who is a processor, and such a service requires the collection and/or processing of PI belonging to a controller, the supplier or business partner will conclude a data transfer agreement with the group on the terms set out in Annexures A1, A2 and A3 of this policy (which is not negotiable).

The following policy statement relates only to the provision of cloud services, where in scope:

5.1.8 Where the supplier is a cloud service provider, the group will provide to the supplier its cloud services-specific terms and conditions, which will be incorporated into the agreement with the supplier.

5.2 Processing limitation

5.2.1 The supplier or business partner will, as far as possible, collect PI directly from the data subject to whom the PI relates unless: the information is contained in or derived from a public record; or deliberately made public by the data subject; or the data subject has consented thereto; or it is in the legitimate interest of the data subject or the group; or collection from another source is legally required; or needed for court proceedings or national security; or otherwise directed in writing by the group; or such PI and/or record is provided by the group.

5.2.2 The supplier or business partner will process PI of data subjects lawfully and in a reasonable manner so that it does not unreasonably intrude on the data subject's right to privacy. The supplier or business partner will ensure that, where legally necessary for a particular processing action, consent is collected from the data subject as per the instructions provided by the group, and that such consent will be retained as per records management best practice principles.

5.2. Purpose specification

5.2.3 The supplier or business partner shall collect PI and/or records only as far as such PI is necessary for the supplier or business partner to comply with the agreement, or for the exercise of the supplier's rights or instructions in terms of the agreement with the group.

5.2.4 The group requires the supplier or business partner to maintain all PI and/or records for the period required by the applicable legislation and to keep an up-to-date retention schedule as required by records management principles. The supplier or business partner will be required to maintain the records and apply records management best practice principles to all PI, in accordance with the applicable legislation, irrespective of the form. All retention periods, disposal methods and/or processes must be documented and the evidence of the destruction of all records must be maintained. A copy or applicable extract of the group's records retention and destruction policies will be made available where necessary or required.

5.3 Further processing limitation

5.3.1 The supplier or business partner shall only collect and/or process PI and/or records for the purpose for which it was originally collected and to fulfil all its obligations to the group in terms of its agreement with the group.

5.3.2 If there is a requirement for any further processing of PI and/or records, authorisation from the group will be requested in writing by the supplier or business partner. No reliance may be placed by the supplier or business partner on the exceptions contained in section 15 of POPIA.

5.4 Information quality

5.4.1 The supplier or business partner shall ensure that, where PI is processed in fulfilment of its obligations under any agreement with the group, that such PI is complete, accurate, not misleading and updated where necessary. Should the supplier or business partner become aware of any PI changes, the supplier or business partner must as soon as practically possible inform the group of such changes; and whether a data subject's PI is incomplete, inaccurate or misleading so that the necessary updates are made.

5.5 Openness

5.5.1 If the supplier or business partner collects PI, SPI or children's PI on behalf of the group, the supplier or business partner must notify the data subject from whom the information is being collected, to the extent required by applicable privacy laws, of the following:

- that the supplier or business partner is acting on behalf of the group;
- what information is being collected;
- the purpose of the collection of that information;
- any legal requirements for collection;
- whether the supply of the information is voluntary or mandatory;
- the consequences for failure to supply such information;
- the name and address of the responsible party;
- where applicable, whether the responsible party intends to transfer the information across a border or borders, to another country and the level of protection afforded the information by that country;
- the right of the data subject to access and correct the PI; and

- any further information as required by the group (such as the recipients of the information, existence of the right to access/rectify the information, existence of the right to object to the processing of the information, and the right to lodge a complaint to the Information Regulator and its contact details).

5.5.2 All employees, agents and subcontractors of the supplier or business partner shall take reasonable steps to identify themselves to a data subject who has been contacted. Further to that, the data subject must be informed that the said supplier or business partner is acting on behalf of the group.

5.6 Security safeguards

5.6.1 The supplier or business partner shall secure the integrity and confidentiality of all PI and/or records in its possession by putting appropriate, reasonable, technical and organisational measures in place to prevent loss or unauthorised destruction of PI, as well as to prevent unlawful access to or processing of PI in the supplier's or business partner's possession.

5.6.2 The supplier or business partner must complete the group PI third-party privacy assessment prior to the conclusion of the agreement. The control environment must be agreed upon with the group prior to the commencement of the engagement.

5.6.3 The supplier and business partner are prohibited from disclosing or transferring PI and/or records to any external third party, except for the purposes of fulfilling their obligations in terms of the relationship with the group; or unless otherwise directed to do so by the group in writing; or unless otherwise required by law.

5.6.4 Where the supplier or business partner is requested to disclose PI and/or records for a purpose not authorised under the agreement with the group, or if disclosure is required by law, then the supplier or business partner will immediately notify the group regarding the request or demand disclosure in writing, and must not disclose the PI unless directed to do so in writing by the group, or unless otherwise required by law. Where disclosure is required by law, the supplier or business partner will, where possible, provide the group with reasonable written notice of such requirement in order to provide the group with an opportunity to exercise its rights, and will only disclose such PI and/or records as it is strictly required to disclose by law.

5.6.5 The supplier or business partner shall identify all reasonably foreseeable internal and external risks to PI in the fulfilment of its obligations in terms of the agreement with the group. Appropriate safeguards must be established and maintained against the identified risks. Regular verification of the effective implementation of such safeguards and continual review and updates of safeguards in response to new risks must be undertaken by the supplier and business partner. Records of the reviews must be retained.

5.6.6 The group may, at any time and upon reasonable notice to the supplier or business partner, enter the premises of the supplier or business partner to inspect or audit, or request a third party to audit the supplier's or business partner's compliance with this policy. This includes but is not limited to security and information management requirements under the provisions of privacy legislation and/or the terms and conditions of the agreement as concluded between the supplier or business partner and the group. The supplier or business partner is required to cooperate with any such audit or inspection.

5.6.7 The supplier or business partner must notify the responsible party (the group) immediately where there are reasonable grounds to believe that the PI that it processes on behalf of the group has been accessed or acquired by any unauthorised person or entity.

5.6.8 The group will nominate a contact person to receive such privacy incidents, which will also be specified in the agreement.

5.6.9 At the time of the privacy incident, the supplier or business partner must report the privacy incident information to the group as per Annexure B.

5.6.10 The group will put in place internal processes and procedures with clearly defined roles and responsibilities. This will ensure that the discovery or identification, recording and management of security compromises as they arise, are in line with its internal privacy incident management plan.

5.6.11 In the event that the supplier or business partner handles or processes payment card information on behalf of the group, they must at all times fully comply with the relevant and current standard as outlined in the Payment Card Industry Data Security Standard (PCI DSS) (www.pcisecuritystandards.org) to ensure continuous protection of sensitive cardholder data. The supplier or business partner will at all times be responsible for security when processing and transmitting card information and PI. The group may, as and when required, request proof of compliance to PCI DSS.

5.7 Data subject participation

5.7.1 A data subject has the right to, after providing adequate proof of identity and after payment of any fee required by law (if applicable):

- enquire if PI about them has been collected by the supplier or business partner on behalf of the group;
- enquire how the PI is being used by the supplier or business partner whilst acting on behalf of the group;
- enquire whom the information has been disclosed to by the supplier or business partner whilst acting on behalf of the group;
- challenge the accuracy and completeness of PI in the possession of the supplier or business partner who is acting on behalf of the group;
- object to the processing of such PI by the supplier or business partner who is processing on behalf of the group; and
- withdraw their consent to the processing of their PI by the supplier or business partner who is processing on behalf of the group.

5.7.2 The supplier or business partner must immediately direct any requests by a data subject to access and/or amend any PI, or requests to withdraw consent to the processing of their PI that the supplier or business partner holds on behalf of the group, to the group to be handled in terms of the group's PAIA manual and process.

6 AUDIT AND INSPECTION OF PI AND RECORDS

6.1 Prior to the conclusion of any agreement with any supplier or business partner that will process PI and/or records on behalf of the group, the group may conduct a third-party privacy assessment when required.

6.2 The group reserves the right to audit, upon providing the supplier with reasonable notice of the said audit, the controls implemented by the supplier and business partner throughout the duration of the agreement, as a measure of continued due diligence or privacy risk mitigation on the part of the group.

6.3 The group reserves the right to audit:

- the supplier's or business partner's adherence to privacy principles, as well as security, information and records management practices, but most importantly the supplier's or business partner's compliance with the policy requirements set out herein; and
- the PI and/or records that the supplier or business partner holds on behalf of the group in performance of its obligations towards the group.

7 CROSS-BORDER TRANSFER

7.1 In cases where the supplier or business partner (or any of its subcontractors) is domiciled outside the Republic of South Africa, or transfers PI and/or records outside the Republic of South Africa whilst collaborating with or providing the group with goods and/or services, such information may only be transferred in terms of the agreement with FirstRand.

7.2 Where the processing of PI occurs in a country which has legislation more stringent than POPIA, then the more stringent legislation's provisions will be applicable to the processing of such personal information.

7.3 The supplier and business partner may not transfer PI that is being processed on behalf of the group outside the borders of the Republic of South Africa unless:

- the supplier, business partner or third party who is receiving the information is subject to a PI protection law, binding corporate rules or binding agreement rules that effectively uphold the principles of reasonable processing and contain provisions that have substantively similar provisions to POPIA regarding transfer of PI to foreign jurisdictions;
- the data subject has provided consent for the transfer;
- the transfer of such PI is required for the performance of a contract between the data subject and the group;
- the transfer of such PI is necessary for the performance of a contract concluded between the group and a third party, in the interest of the data subject;
- the transfer of such PI is for the benefit of the data subject and it is not practical to obtain consent and the data subject would have provided such consent had the data subject been able to; or
- with the prior written approval of the group.

8 NOTIFICATIONS BY SUPPLIER OR BUSINESS PARTNER TO THE GROUP

8.1 All notifications to the group relating to access to PI and/or records in the possession of a supplier or business partner that contain PI but belong to the group, shall be addressed to the group in writing.

8.2 These notifications include notifications to comply with requests from the Information Regulator in terms of POPIA compliance; requests for access to PI; requests to address complaints from the Information Regulator; and requests to access information, in terms of PAIA, that is the property of the group.

9 THIRD-PARTY MANAGEMENT

9.1 The supplier or business partner must inform the group in writing, prior to engaging the services of a third party or subcontractor, to assist in providing services in terms of the main agreement with the group. The group may approve or decline the use of such third party or subcontractor.

9.2 Where the group approves the appointment of such third party or subcontractor, the supplier or business partner shall provide the group with written confirmation of such appointment, which includes the identity and location of such third party or subcontractor.

9.3 The supplier or business partner may only disclose PI and/or records to third parties under the following circumstances:

- in the case that the supplier or business partner has contracted with a third party to provide goods and/or services on behalf of the supplier or business partner in order for the supplier or business partner to perform its obligations under the agreement with the group;
- has the consent of the data subject;
- to protect the legitimate interest of the data subject;
- to pursue the legitimate interest of the group;
- to pursue the legitimate interest of a third party; or
- in cases where the supplier or business partner is under a legal duty to share PI and/or records, to comply with a legal obligation.

9.4 In sharing this information, the supplier or business partner shall ensure that the third party provides the same level of protection to the PI as required by this policy, the agreement with the group and applicable PI protection laws. The contract between the third party and/or supplier or business partner must adhere to the requirements contained in this policy. For the purposes of this section, "third party" means any person or entity other than the supplier and/or operator, the group or other persons authorised by the group to process PI for the responsible party, this being the group.

10 TERMINATION EXPECTATIONS

10.1 At termination of the agreement, the supplier or business partner will, at the direction of the group:

- return to the group all PI and/or records that contain PI that belong to the group that were created throughout the duration of the agreement, including PI and/or records that were provided to the supplier and business partner at the inception of the engagement with the group, irrespective of when they were created or provided; or
- provide the group with the destruction certificate indicating that all PI and/or records that contain PI that were the possession of the supplier or business partner have been destroyed; and
- ensure that all PI and/or records in the possession of a third party (as defined in paragraph 9.4) or subcontractor are returned to the group.

11 GENERAL

The group reserves its right to enforce its rights as stated in the agreement between the group and the supplier or business partner if the supplier or business partner fails to comply with the provisions of this policy or the applicable legislation provisions. Failure to comply with the provisions of this policy may, without limitation, result in legal action and/or termination of the master agreement with the group.

12 OWNERSHIP AND REVIEW

This policy is owned by FirstRand Group Compliance and must be reviewed at least every two years. This policy will also be reviewed when any applicable code of conduct under POPIA is published or there is any amendment to any overarching legislation.

-END-

ANNEXURE A1

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

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

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

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

(i) where it has obtained the data subject's prior consent;

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

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

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

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

8.4 Storage limitation

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

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

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

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

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

8.6 Sensitive data

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

8.7 Onward transfers

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

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

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

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

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

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

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

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

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

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

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

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

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the

data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In

addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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

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

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

MODULE FOUR: Transfer processor to controller

8.1 Instructions

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

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

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

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

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data[7], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

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

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

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

8.3 Documentation and compliance

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

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

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

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

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

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

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

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

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

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

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

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

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

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

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

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

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

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

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

MODULE FOUR: Transfer processor to controller

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

Clause 11

Redress

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

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[11] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

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

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

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

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

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

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

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

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[12];

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

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

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

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

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

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

Clause 15

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

15.1 Notification

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

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall

include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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

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

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of 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.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country

to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

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

MODULE FOUR: Transfer processor to controller

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

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

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

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

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

1. Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

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

1. Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

……..

Categories of personal data transferred

……..

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

……..

The frequency of the transfer (e.g. whether the data 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 data 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

……..

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

……

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

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

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

[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 organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

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 minimisation

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 organisational 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

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

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

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 authorised): …

2. …

ANNEXURE A2

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):

Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): 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?
1						
2						
3						
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

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: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

Interpretation of this Addendum

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

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

	including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

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

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

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

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

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

Alternative 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.

ANNEXURE A3

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

This IDTA 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 and signatures

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title:	Full Name (optional): Job Title:

	Contact details including email:	Contact details including email:
Importer Data Subject Contact		Job Title: Contact details including email:
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed: Date of signature: Full name: Job title:	Signed for and on behalf of the **Importer** set out above Signed: Date of signature: Full name: Job title:

Table 2: Transfer Details

UK country's law that governs the IDTA:	☐ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☐ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☐ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☐ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)

Whether UK GDPR applies to the Importer	☐ UK GDPR applies to the Importer's Processing of the Transferred Data ☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: Date of agreement: Parties to the agreement: Reference (if any): **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: Date of agreement: Parties to the agreement: Reference (if any): **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: Date of agreement: Parties to the agreement: Reference (if any):
Term	The Importer may Process the Transferred Data for the following time period: ☐ the period for which the Linked Agreement is in force ☐ time period:

	☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	☐ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. ☐ the Parties can end the IDTA before the end of the Term by serving: [ ] months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ☐ Importer ☐ Exporter ☐ neither Party
Can the Importer make further transfers of the Transferred Data?	☐ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: [ ] ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☐ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: [ ]

	The Parties must review the Security Requirements at least once: ☐ each _____ month(s) ☐ each quarter ☐ each 6 months ☐ each year ☐ each _____ year(s) ☐ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ☐ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of uniquely identifying a natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☐ none of the above ☐ set out in:

	And: ☐ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ☐ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Purpose	☐ The Importer may Process the Transferred Data for the following purposes: ☐ The Importer may Process the Transferred Data for the purposes set out in: In both cases, any other purposes which are compatible with the purposes set out above. ☐ The purposes will update automatically if the information is updated in the Linked Agreement referred to. ☐ The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

Security of Transmission	

Security of Storage	
Security of Processing	
Organisational security measures	
Technical security minimum requirements	
Updates to the Security Requirements	☐ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☐ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	

(iii) Extra contractual protections	

Part 3: Commercial Clauses

Commercial Clauses	

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date

and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate

considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to

ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

16.1.2 the third party has been added to this IDTA as a Party; or

16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references

to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving

Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

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

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and

- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);

- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	**Legal definition (this is how this word or phrase must be interpreted in the IDTA)**
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: • a territory; • one or more sectors or organisations within a third country; • an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	Act 2018 on 2 February 2022, as it is revised under Section 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.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 5.4 of those Mandatory Clauses.

ANNEXURE B

Reporting of privacy incidents by suppliers and business partners

(a) Reporter information

Name, surname, employee number, email address, mobile phone number of person reporting the privacy incident.

(b) Description of the privacy incident circumstances

1. Root cause information relating to the privacy incident. The root cause should be further classified according to external causal factors (e.g. phishing attacks, denial of services); people causal factors (e.g. unauthorised activity by internal or external staff in relation to the PI); governance causal factors (e.g. no proper escalation processes and lack of proper oversight in relation to PI processing activities); process causal factors (e.g. inefficient/ineffective process design or inadequate or ineffective procedures in relation to the exchange of PI with third parties); and technology, infrastructure, facilities causal factors (e.g. inadequate data/system security, including access/protection/configuration).
2. Does the privacy incident involve identifiable PI or is the PI anonymised?
3. Date of the privacy incident.
4. Who was the privacy incident reported to?
5. Systems involved?
6. How many (volume of) records affected?
7. How many customers/data subjects affected?
8. Does the privacy incident include special personal information or sensitive information of a data subject?
9. Group operating business/customer segments/business unit(s) affected.
10. Confirmation of the number of group customers impacted, emanating from the compromised group data.
11. Provide a list of the affected data fields, emanating from the compromised group data.
12. Provide a proposed remediation plan for the data breach.
13. Provide a brief description of the potential service disruptions anticipated from the supplier and/or business partner as a result of the data breach, including interim plans to manage the disruption.

(c) Remediation actions

1. Information relating to the remedial actions undertaken by the supplier or business partner. Such actions should be described in detail.
2. The supplier and/or business partner must provide assurance that when a privacy incident occurs, the incident has been reported to FirstRand in terms of the agreed timelines, set out in the agreement.
3. The supplier and/or business partner must provide assurance that, where the supplier and/or business partner is an operator of the group, they will cooperate and provide the group with the requisite information to enable FirstRand to report such breach to relevant regulators and/or authorities. The supplier and/or business partner will not be permitted to release any communications or notifications without FirstRand's approval and consent.
4. The supplier and/or business partner must provide assurance that, where it is a joint responsible party or joint data controller with the group, it will collaborate and cooperate with FirstRand and agree on communications disclosed to regulators and the public.

(d) Non-compliance to privacy law and/or other legislation

Specify which sections in the applicable privacy legislation has been breached.