tag.

Digital Interact (“DI”) Subscription

and Related Services

DATA PROTECTION ADDENDUM

Contents

This Data Protection Addendum ("**DPA**") forms part of the Tag Digital Interact General Terms and Conditions for Subscribed Services Agreement or any other agreement between Tag and Customer for the purchase of Services from Tag that references this DPA (the "**Agreement**"). Notwithstanding the foregoing, in the event of a conflict or inconsistency between the terms of the Agreement and this DPA, this DPA shall prevail.

This DPA shall be effective from the Effective Date of the Agreement, as applicable. Except as modified below the terms of the Agreement shall remain in effect.

1 Definitions

1.1 In this DPA, defined terms shall have the same meaning, and the same rules of interpretation shall apply as in the remainder of the Agreement. In addition, the following definitions have the meanings given below:

Adequacy Finding	refers to a legally-binding decision issued by the applicable authority allowing the transfer of Personal Data to a third country which has been considered adequate in terms of data protection safeguards under (i) an implementing act adopted in accordance with the examination procedure referred to in GDPR Article 93(2) and/or (ii) Schedule 21 of the UK Data Protection Act 2018;
Applicable Law	means applicable laws of the United Kingdom (UK), the European Union (EU), the European Economic Area (EEA) or any of the EU or EEA's member states from time to time together with applicable laws in the United Kingdom from time to time*;*
Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws, as amended or updated from time to time;
Data Protection Laws	means all Applicable Laws relating to the Processing, privacy and/or use of Personal Data, as applicable to either party or the Services, including, but not limited to, the following laws to the extent applicable in the circumstances: (a) the EU GDPR; (b) the UK GDPR and the Data Protection Act 2018; (c) any other laws to which the processing or use of Personal Data applies; (d) any laws which replace, extend, re-enact, consolidate or amend any of the foregoing;
Data Protection Losses	means all liabilities, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
GDPR	means the EU GDPR and UK GDPR, as applicable in the context;
Effective Date	means the effective date in (a) Tag's General Terms and Conditions for Subscribed Services Agreement; or (b) any other agreement between Tag and Customer for the purchase of Services which makes reference to this DPA;
EU GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679 as amended, nationally implemented or supplemented from time to time;
EU Standard Contractual Clauses or 'EU SCCs'	means the standard contractual clauses adopted by the European Commission decision on 4 June 2021 governing the transfers of personal data to a Third Country without an Adequacy Finding;
Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Personal Data;
Processing Instructions	has the meaning given to that term in paragraph 3.1.1;
Sub-Processor	means another Processor engaged by Tag for carrying out Processing activities in respect of the Personal Data on behalf of the Customer;
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
UK	means the United Kingdom;
UK GDPR	means the EU GDPR and the Data Protection Act 2018 as both amended by the UK Data Protection Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019(2019/419), together with any laws and regulations that replaces or amends any of these from time to time;
UK Standard Contractual Clauses or 'UK SCCs'	means the standard contractual clauses recognised under the UK GDPR, as a means of providing appropriate safeguards for Personal Data transferred out of the United Kingdom, as amended, replaced or supplemented from time to time.

The following terms shall have the same meanings as in the Data Protection Laws, and their equivalent terms (and their derivatives) shall be construed accordingly: **"controller"**, **"data protection officer"**, **"Personal Data"**, **"processor"**, **"processing"**, **"data subject"**, **"international organisation"**, **"Member State"**, **"supervisory authority"**, **"Third Country"**, and **"Union".**

2 Processor and Controller

2.1 The parties agree that, for the Personal Data, the Customer shall be the Controller and Tag shall be the Processor. Nothing in the Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.

2.2 To the extent the Customer is not sole Controller of any Personal Data it warrants that it has full authority and authorisation of all relevant Controllers to instruct Tag to process the Personal Data in accordance with the Agreement.

2.3 Tag shall process Personal Data in compliance with:

2.3.1 the obligations of Processors under Data Protection Laws in respect of the performance of its and their obligations under the Agreement; and

2.3.2 the terms of the Agreement.

2.4 The Customer shall ensure that it, its Affiliates and each Authorised User shall at all times comply with:

2.4.1 all Data Protection Laws in connection with the Processing of Personal Data, the use of the Services (and each part) and the exercise and performance of its respective rights and obligations under the Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.4.2 the terms of the Agreement.

2.5 The Customer warrants, represents and undertakes, that at all times:

2.5.1 all Personal Data (if processed in accordance with the Agreement) shall comply in all respects, including in terms of its collection, storage and Processing, with Data Protection Laws;

2.5.2 fair Processing and all other appropriate notices have been provided to the Data Subjects of the Personal Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by Data Protection Laws in connection with all Processing activities in respect of the Personal Data which may be undertaken by Tag and its Sub-Processors in accordance with the Agreement;

2.5.3 the Personal Data is accurate and up to date;

2.5.4 it shall establish and maintain adequate security measures to safeguard the Personal Data in its possession or control from (including from unauthorised or unlawful destruction, corruption, Processing or disclosure) and maintain complete and accurate backups of all Personal Data provided to Tag (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Personal Data in the event of loss, damage or corruption of such Personal Data by Tag or any other person;

2.5.5 all instructions given by it to Tag in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

2.5.6 it has undertaken due diligence in relation to Tag's Processing operations and commitments and it is satisfied (and all times it continues to use the Services remains satisfied) that:

(a) Tag's Processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage Tag to process the Personal Data;

(b) the technical and organisational measures set out in the Agreement (each as updated from time to time) shall ensure a level of security appropriate to the risk with regards to the Personal Data; and

(c) Tag has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

3 Instructions and details of Processing

3.1 Insofar as Tag processes Personal Data on behalf of the Customer, Tag:

3.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Personal Data only on and in accordance with the Customer's documented instructions as set out in this paragraph 3.1 and paragraphs 3.2 and 3.3 as updated from time to time;

3.1.2 if Applicable Law requires it to process Personal Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before Processing the Personal Data (unless Applicable Law prohibits such information on important grounds of public interest); and

3.1.3 shall promptly inform the Customer if Tag becomes aware of a Processing Instruction that, in Tag's opinion, infringes Data Protection Laws, provided that:

(a) this shall be without prejudice to paragraphs 2.4 and 2.5; and

(b) to the maximum extent permitted by Applicable Law, Tag shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any Processing in accordance with the Customer's Processing Instructions following the Customer's receipt of the information required by this paragraph 3.1.3.

3.2 The Customer acknowledges and agrees that the execution of any computer command to process (including deletion of) any Personal Data made in the use of any of the Subscribed Services by an Authorised User will be a Processing Instruction (other than to the extent such command is not fulfilled due to technical, operational or other reasons, including as set out in the Training Materials). The Customer shall ensure that Authorised Users do not execute any such command unless authorised by the Customer (and by all other relevant Controller(s)) and acknowledges and accepts that if any Personal Data is deleted pursuant to any such command Tag is under no obligation to seek to restore it.

3.3 Subject to the Order Form the Processing of the Personal Data by Tag under the Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in Appendix 1.

4 Technical and Organisational Measures

4.1 Taking into account the nature of the Processing, Tag shall implement and maintain, at its cost and expense, the Technical and Organisational Measures in relation to the Processing of Personal Data by Tag.

5 Using staff and other Processors

5.1 The Customer grants Tag a general authorisation to appoint Sub-Processors for the Processing of Personal Data.

5.2 Tag shall:

5.2.1 prior to the relevant Sub-Processor carrying out any Processing activities in respect of the Personal Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under paragraphs 2 to 11 (inclusive) (including those obligations relating to sufficient guarantees to implement appropriate technical and organisational measures); and

5.2.2 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.3 Tag shall ensure that all persons authorised by it (or by any Sub-Processor) to process Personal Data are subject to a binding written contractual obligation to keep the Personal Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Tag shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

6 Assistance with Compliance and Data Subject Rights

6.1 Tag shall assist the Customer, by implementing appropriate technical and organisational measures, to comply with the Customer's obligation to respond to all Data Subject Requests it receives under Data Protection Laws. The Customer shall pay Tag for all work, time, costs and expenses incurred in connection with such activity, calculated on a time and materials basis at Tag's rates set out in Tag's Standard Pricing Terms, a copy of which shall be available to the Customer upon request.

6.2 Tag shall provide such assistance as the Customer reasonably requires (taking into account the nature of Processing and the information available to Tag) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

6.2.1 security of Processing;

6.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

6.2.3 prior consultation with a Supervisory Authority regarding high risk Processing; and

6.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay Tag for all work, time, costs and expenses incurred in connection with providing the assistance in this paragraph 6.2, calculated on a time and materials basis at Tag's rates set out in Tag's Standard Pricing Terms.

7 International Data Transfers

7.1 The Customer hereby authorises Tag to process Personal Data, including using Sub-Processors, in accordance with this Agreement, outside the country in which the Customer is located by way, as necessary, of Appropriate Safeguards and in accordance with Data Protection Laws, an Adequacy Finding, and the Agreement. The provisions of the Agreement (including this Data Protection Addendum) shall constitute the Customer's instructions with respect to transfers in accordance with paragraph 3.1.1.

7.2 Restricted Transfers Subject to UK GDPR:

7.2.1 Where any Personal Data transfer between Customer and Tag requires execution of the UK SCCs in order to comply with UK GDPR, (where Customer is the entity exporting Personal Data of UK data subjects to Tag located outside the UK or third county without an Adequacy Finding) the Customer (as '**data exporter'**) and the Tag (as '**data importer'**) will enter into the UK SCCs as set out in this DPA and shall take all other actions required to legitimise the transfer.

7.2.2 If, after the date of this DPA, the Information Commissioners Office ("**ICO**") publishes new clauses which replace the UK SCCs so that the UK SCCs are no longer a lawful transfer mechanism recognised under the UK GDPR, Parties agree to replace the UK SCCs attached hereto with an executed copy of the new clauses. The Parties shall take all actions required to implement such new clauses and such new clauses shall apply to the Personal Data processed under the Agreement from the date of their execution and thereafter. A reasonable delay in performing and/or executing such actions will not invalidate or render the DPA or the existing transfer mechanism unenforceable.

7.3 Restricted Transfers Subject to the EU GDPR:

7.3.1 Where any Personal Data transfer between Customer and Tag requires execution of the EU SCCs in order to comply with the EU GDPR (where the Customer is the entity exporting Personal Data of EU data subjects to a Tag entity outside the EEA or third county without an Adequacy Finding) the Customer (as '**data exporter'**) and the Tag (as '**data importer'**) will enter into the EU SCCs as set out in this DPA and shall take all other actions required to legitimise the transfer.

7.4 The Customer acknowledges that due to the nature of cloud services, the Personal Data may be Transferred to other geographical locations in connection with use of the Service further to access and/or computerised instructions initiated by Authorised Users. The Customer acknowledges that Tag does not control such Processing and the Customer shall ensure that Authorised Users (and all others acting on its behalf) only initiate the Transfer of Personal Data to other geographical locations if Appropriate Safeguards are in place and that such Transfer is in compliance with all Applicable Laws.

8 Information and Audit

8.1 Tag shall maintain, in accordance with Data Protection Laws binding on Tag, written records of all categories of Processing activities carried out on behalf of the Customer.

8.2 On request, Tag shall provide the Customer (or an independent third party auditor reasonably acceptable to Tag) with a copy of the third-party certifications and audits to the extent made generally available to its customers. Such information shall be confidential to Tag and shall be Tag Confidential Information as defined in the Agreement, and shall be treated in accordance with applicable terms.

8.3 In the event that the Customer, acting reasonably, deems the information provided in accordance with paragraph 8.2 insufficient to satisfy its obligations under Data Protection Laws, Tag shall, on request by the Customer make available to the Customer such information as is reasonably necessary to demonstrate Tag's compliance, its obligations under this Agreement and Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or an independent third party auditor reasonably acceptable Tag) for this purpose, provided:

8.3.1 such audit, inspection or information request is reasonable, limited to information in Tag's possession or control and is subject to the Customer giving Tag reasonable (and in any event at least sixty (60) days) prior notice of such audit, inspection or information request;

8.3.2 the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the frequency, timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which the Customer or third party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure Tag is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this paragraph 8.3);

8.3.3 the Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of Tag;

8.3.4 the duration of any audit or inspection shall be limited to one Business Day;

8.3.5 all costs of such audit or inspection or responding to such information request shall be borne by the Customer, and Tag's costs, expenses, work and time incurred in connection with such audit or inspection shall be reimbursed by the Customer on a time and materials basis in accordance with Tag's Standard Pricing Terms;

8.3.6 the Customer's rights under this paragraph 8.3 may only be exercised once in any consecutive 12 month period, unless otherwise required by a Supervisory Authority or if the Customer (acting reasonably) believes Tag is in breach of this Data Protection Addendum;

8.3.7 the Customer shall promptly (and in any event within one Business Day) report any non-compliance identified by the audit, inspection or release of information to Tag;

8.3.8 the Customer agrees that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits shall be Tag Confidential Information as defined in the Agreement, and shall be treated in accordance with applicable terms;

8.3.9 the Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any third party auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of Tag while conducting any such audit or inspection; and

8.3.10 this paragraph 8.3 is subject to paragraph 8.4.

8.4 The Customer acknowledges and accepts that relevant contractual terms agreed with Sub-Processor(s) may mean that Tag or Customer may not be able to undertake or facilitate an information request or audit or inspection of any or all Sub-Processors pursuant to paragraph 8.3. The Customer's rights under paragraph 8.3 shall not apply to the extent inconsistent with relevant contractual terms agreed with Sub-Processor(s) and paragraphs 5.2.1 and 8.3 shall be construed accordingly. Notwithstanding this, Tag shall ensure that it has appropriate mechanisms in place to ensure its Sub-Processors meet their obligations under Data Protection Laws and Tag's obligations under the Agreement and the Customer accepts that the provisions of this paragraph 8.4 shall satisfy Tag's obligations in this regard. To the extent any information request, audit or inspection of any Sub-Processor are permitted in accordance with this 8.4, equivalent restrictions and obligations on the Customer to those in paragraphs 8.3.1 to 8.3.10 (inclusive) shall apply together with any additional or more extensive restrictions and obligations applicable in the circumstances.

9 Breach Notification

9.1 In respect of any Personal Data Breach involving Personal Data, Tag shall, without undue delay:

9.1.1 notify the Customer of the Personal Data Breach; and

9.1.2 provide the Customer with details of the Personal Data Breach under Data Protection Laws to enable the Customer to make a reasonable determination with respect the Breach.

9.1.3 taking into account the nature of the processing, assist Customer (at the Customer's reasonable cost) by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to the data subject request under the Data Protection Laws.

9.1.4 provide the Customer with additional and supplementary details of the Personal Data Breach as they become aware of them.

10 Deletion of Personal Data and copies

10.1 Following the end of the provision of the Services (or any part) relating to the Processing of Personal Data Tag shall, at the cost and choice of the Customer, dispose of Personal Data in accordance with its obligations under the Agreement unless Data Protection Laws requires the storage and/or retention of such Personal Data.

10.2 Tag shall have no liability (howsoever arising, including in negligence) for any deletion, destruction or retention (if required to do so under Data Protection Laws) of any such Personal Data undertaken in accordance with the Agreement.

For and On Behalf of	For and On Behalf of
TAG WORLDWIDE TECH LIMITED	**[CLIENT NAME]**
Signature:	Signature:
Name:	Name:
Date:	Date:

APPENDIX 1
DATA PROCESSING DETAILS

Subject-matter of Processing:	*The subject matter of the Processing is the Customer Personal Data* in accordance with the relevant Order Form and under the Agreement.
Duration of the Processing:	*The duration of the Processing is until the earlier of final termination or final expiry of the Agreement, except as otherwise expressly stated in the Agreement;*
Nature and purpose of the Processing:	*Processing as reasonably required to provide the Services in accordance with the Agreement, as further initiated, requested or instructed by Authorised Users in connection with their use of the Services, or by the Customer, in each case in a manner consistent with the Agreement and in relation to each Subscribed Service, in accordance with the nature and purpose identified in the relevant Order Form.*
Type of Personal Data:	*[Name, Email Address, Job Title, Bank Details, etc.]*
Categories of Data Subjects:	*[Employees, Customer's Employees, Customer's Customers/Clients, Consumers, Children]*
Special categories of Personal Data:	*[E.g. Sexuality, Criminal Records, Trade Union Membership]*

APPENDIX 2

TECHNICAL AND ORGANISATIONAL MEASURES

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

Security

Tag and its group of companies has adopted an Information Security Policy which details the technical and organisational security measures implemented by the data exporters and the data importers and accommodates the requirements of its specific Customer engagements. The Information Security Policy is kept under regular review and is updated as required by technological or contractual demands. Below is a summary of the key features of the Information Security Policy as at the date of this Agreement.

1. Data Classification Scheme

A Data Classification Scheme is used to protect physical and logical assets and to ensure a consistent and appropriate method of handling, storing and protecting these assets, according to their level of sensitivity.

2. Physical Access Controls

Access to company premises is controlled and provided on an individual and accountable basis. Measures are implemented to ensure that access is only provided to individuals that have been accessed ID badges or visitor badges. Access to secured areas such as server rooms are restricted to authorised personnel only, and visitors must follow additional procedures in place for gaining access.

3. Logical Access Controls

Access to company IT systems and software applications is provided on an individual and accountable basis. Approved users are issued with unique credentials, which must not be shared with or communicated to any other person. Access rights are regularly reviewed to ensure that only those persons who require access to systems are provided with such access. Access to systems is granted according to the principle of least privilege.

4. Cryptographic Techniques

Encryption techniques must be applied to data in accordance with the Data Classification Scheme.

5. Removable Media

Write access to USB removable storage devices, removable hard disks and CD & DVD drives is disabled by default in many locations.

6. Monitoring

The company may monitor use of IT systems (including internet and email) and telecommunications systems for the purposes of detecting infringements of its policies.

APPENDIX 3

UK STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of the UK GDPR for the transfer of personal data to processors established in Third Countries which do not have an Adequacy Finding.

For the purposes of this Appendix 3, references to the "**data exporter**" shall mean the Customer and "**data importer**" shall mean Tag (each a "**party**", together the "**parties**").

Clause 1
Definitions

For the purposes of the Clauses:

(a) '**personal data'**, '**special categories of data'**, '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**Commission**' shall have the same meaning as in as in the UK GDPR;

(b) '**The Data Exporter**' means the controller who transfers the personal data;

(c) '**The Data Importer**' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018 ;

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

(e) '**The Applicable Data Protection Law**' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK

(f) '**Technical And Organizational Security Measures**' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

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

Clause 3
Third-party beneficiary clause

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

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

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

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

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

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

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

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Annex 3B to this contract;

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

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

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commission if the data exporter decides to continue the transfer or to lift the suspension;

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

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

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

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organizational security measures specified in Annex B before processing data transferred;

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

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

  (ii) any accidental or unauthorized access; and

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

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

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by

the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner ;

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

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

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

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

Clause 6
Liability

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

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

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

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

Clause 7
Mediation and jurisdiction

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

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

   (b) to refer the dispute to the UK courts.

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

Clause 8
Cooperation with the Commissioner

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

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

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

Clause 9
Governing law

The Clauses shall be governed by the law of the country in which the data exporter is established, namely the United Kingdom.

Clause 10
Amendment of the contract

The parties undertake not to vary or modify the Clauses without prior written consent and that such variance and/or modification shall not be in contravention of applicable data protection laws. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

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

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

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the United Kingdom where the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12
Obligation after the termination of personal data-processing services

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

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

On behalf of	On behalf of
the Data Exporter, **Customer:**	the Data Importer, **Tag:**
Signature:	**Signature:**
Name:	**Name:**
Position:	**Position:**
Date:	**Date:**

ANNEX 3A

TO THE UK STANDARD CONTRACTUAL CLAUSES

This Annex 3A forms part of the UK Standard Contractual Clauses and must be completed and signed by the parties

The United Kingdom may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex 3A

Data exporter	The data exporter is (please specify briefly your activities relevant to the transfer): [relevant activities]…
Data importer	The data importer is (please specify briefly activities relevant to the transfer): [relevant activities]…
Data subjects	The personal data transferred concern the following categories of data subjects (please specify): [Describe data subjects – e.g. employees, consumers…]
Categories of data	The personal data transferred concern the following categories of data (please specify): [Category of data here…name, address, job title, place of work, images]
Special categories of data (if appropriate)	The personal data transferred concern the following special categories of data (please specify): [Special categories of data here…e.g. racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition…]
Processing operations	The personal data transferred will be subject to the following basic processing activities (please specify): [Processing activity here – description of services under the agreement, hosting, storage, retrieval, use, copying…]

Annex 3B to the UK Standard Contractual Clauses

Technical and Organisational Measures

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

Security
Tag and its group of companies has adopted an Information Security Policy which details the technical and organisational security measures implemented by the data exporters and the data importers and accommodates the requirements of its specific Customer engagements. The Information Security Policy is kept under regular review and is updated as required by technological or contractual demands. Below is a summary of the key features of the Information Security Policy as at the date of this Agreement.

1. Data Classification Scheme
A Data Classification Scheme is used to protect physical and logical assets and to ensure a consistent and appropriate method of handling, storing and protecting these assets, according to their level of sensitivity.

2. Physical Access Controls
Access to company premises is controlled and provided on an individual and accountable basis. Measures are implemented to ensure that access is only provided to individuals that have been accessed ID badges or visitor badges. Access to secured areas such as server rooms are restricted to authorised personnel only, and visitors must follow additional procedures in place for gaining access.

3. Logical Access Controls
Access to company IT systems and software applications is provided on an individual and accountable basis. Approved users are issued with unique credentials, which must not be shared with or communicated to any other person. Access rights are regularly reviewed to ensure that only those persons who require access to systems are provided with such access. Access to systems is granted according to the principle of least privilege.

4. Cryptographic Techniques
Encryption techniques must be applied to data in accordance with the Data Classification Scheme.

5. Removable Media
Write access to USB removable storage devices, removable hard disks and CD & DVD drives is disabled by default in many locations.

6. Monitoring
The company may monitor use of IT systems (including internet and email) and telecommunications systems for the purposes of detecting infringements of its policies.

APPENDIX 4

EU STANDARD CONTRACTUAL CLAUSES

Clause 1
Purpose and scope

a) The purpose of these modified standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**General Data Protection Regulation**) for the transfer of personal data to a third country without an Adequacy Finding.

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 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 A and/or Annex C (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 4A.

d) 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 Annexes. 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 8.5 (e) and Clause 8.9(b);
iii. Not used;
iv. Clause 12(a) and (d);
v. Clause 13;
vi. Clause 15.1(c), (d) and (e);
vii. Clause 16(e);
viii. Clause 18(a) and (b);

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

Clause 4
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 4A.

Clause 7
Docking clause

a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 4A.

b) Once it has completed the Appendix and signed Annex 4A, 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 4A.

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 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 4A, 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 Annexes 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 Annexes and personal data, the data exporter may redact part of the text of the Annexes 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 4A. 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 the applicable Annexes.

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9
Use of sub-processors

MODULE TWO: Transfer controller to processor

a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [30 days] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10
Data subject rights

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

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.

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

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

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

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

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

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

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

Clause 12
Liability

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

(Delete for Paragraph (a), as appropriate)

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 4A, 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 4A, 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 4A, shall act as competent supervisory authority.]*

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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

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

c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimization

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18
Choice of forum and jurisdiction

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

b) The Parties agree that those shall be the courts of the Republic of Ireland.

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.

On behalf of the Data Exporter, **Customer:**	On behalf of the Data Importer, **Tag:**
Signature:	**Signature:**

Name:	**Name:**
Position:	**Position:**
Date:	**Date:**

Annex 4A to EU Standard Contractual Clauses

This Annex 4A forms part of the Clauses and must be completed and signed by the parties.

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

A. LIST OF PARTIES

Data exporter(s)

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

Name:	
Address:	
Contact person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	
Signature and date:	

Role (controller/processor):	

Data importer(s)

Identity and contact details of the data importer(s), including any contact person with responsibility for data protection

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):	

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	
Categories of personal data transferred:	
Sensitive data transferred (if applicable)	*(Also include all 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

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

Supervisory Authority:	
Country:	
Contact Email:	
Contact Number:	
Address:	

Annex 4B to the EU Standard Contractual Clauses

Technical and Organisational Measures

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

Security
Tag and its group of companies has adopted an Information Security Policy which details the technical and organisational security measures implemented by the data exporters and the data importers and accommodates the requirements of its specific Customer engagements. The Information Security Policy is kept under regular review and is updated as required by technological or contractual demands. Below is a summary of the key features of the Information Security Policy as at the date of this Agreement.

1. Data Classification Scheme
A Data Classification Scheme is used to protect physical and logical assets and to ensure a consistent and appropriate method of handling, storing and protecting these assets, according to their level of sensitivity.

2. Physical Access Controls
Access to company premises is controlled and provided on an individual and accountable basis. Measures are implemented to ensure that access is only provided to individuals that have been accessed ID badges or visitor badges. Access to secured areas such as server rooms are restricted to authorised personnel only, and visitors must follow additional procedures in place for gaining access.

3. Logical Access Controls
Access to company IT systems and software applications is provided on an individual and accountable basis. Approved users are issued with unique credentials, which must not be shared with or communicated to any other person. Access rights are regularly reviewed to ensure that only those persons who require access to systems are provided with such access. Access to systems is granted according to the principle of least privilege.

4. Cryptographic Techniques
Encryption techniques must be applied to data in accordance with the Data Classification Scheme.

5. Removable Media
Write access to USB removable storage devices, removable hard disks and CD & DVD drives is disabled by default in many locations.

6. Monitoring
The company may monitor use of IT systems (including internet and email) and telecommunications systems for the purposes of detecting infringements of its policies.