PICTUREPARK

Data Processing Agreement (DPA)

Last changed: 30 March 2021

This DPA is entered into between Vision Information Transaction and Affiliates (“Picturepark”, “We”, “us” or "our"; the Data Processor) and you (“Customer”, “you”, "your", "yours", “user”; the Data Controller) and is governed by the terms of the Picturepark Cloud Service agreements, and incorporated into other Picturepark agreements.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

“Agreement”	means the agreement between You and us for the provision of Services as defined in the Order Document;
“Authorised Affiliate”	means Your Affiliate(s) who are permitted to use the Services pursuant to the terms of the Agreement, but who have not signed the Agreement or an Order Document;
“Controller”	means You or the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;
“Customer Data”	means all files, content, metadata, Personal Data, Confidential Information and any other data stored or processed via the Services as requested by you as the Controller.
“Data Subject”	shall have the same meaning as in Data Protection Laws or under any equivalent data protection regulation of applicable law. Without limiting the foregoing, Data Subject essentially means a natural person who is the subject of Personal Data.
“Data Protection Laws”	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states, the United Kingdom and Switzerland; any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the Swiss FADP, the UK GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
“DPA”	means this data processing agreement together with its Appendices A, B and C;
“Effective Date”	means the 1st of July 2021 or the date on which you entered into the Agreement, if after the 1st of July 2021 or as mutually defined in the Order Document;
“EU GDPR”	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
“Personal Data”	shall have the same meaning as in Data Protection Laws or under any equivalent data protection regulation of applicable law. Without limiting the foregoing, Personal Data means any information that could be used to identify a natural person, directly or indirectly, in particular by reference to a name or personal identification number, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Personal Data is considered to be Confidential Information;
“Processor”	means us or a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;
“Services”	means our Cloud Service, Technical Support or any Professional Services provided by us to You and Authorised Affiliates;
“Standard Contractual Clauses”	means the EU model clauses for personal data transfer from controllers to processors and third countries as per c2010-593 - Decision 2010/87EU (as attached in Appendix C and amended from time to time, or replaced by subsequent legislation);

"Sub-Processor"	means any person or entity engaged by us or any of our Affiliates to process Customer Data in the provision of the Services to You;
"Swiss FADP"	means the Swiss Federal Act on Data Protection (Swiss FADP) as published in AS 1993 1945;
"UK GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 as implemented into UK law.

2. Purpose

2.1 We have agreed to provide Services to you in accordance with the terms of the Agreement. In providing Services, we shall process Customer Data on behalf of you. Customer Data may include Personal Data. From the Effective Date, we will process and protect such Customer Data in accordance with the terms of this DPA for the term of the Agreement.

3. Scope

3.1 In providing Services to you pursuant to the terms of the Agreement, we shall process Customer Data only to the extent necessary to provide Services in accordance with both the terms of the Agreement and your instructions documented in the Agreement and this DPA, as may be updated from time to time.

3.2 The parties shall take steps to ensure that any natural person acting under their authority respectively who have access to Personal Data do not process Personal Data except on the instructions from you unless he or she is required to do so by any Data Protection Law.

4. Processor Obligations

4.1 We may collect, process or use Customer Data only within the scope of this DPA.

4.2 We confirm that we shall process Customer Data on behalf of you, in accordance with your documented instructions.

4.3 We shall promptly inform you, if in our opinion, any of the instructions regarding the processing of Customer Data provided by you, breach any applicable Data Protection Laws.

4.4 We shall ensure that all employees, agents, officers and contractors involved in the handling of Customer Data: (i) are aware of the confidential nature of the Customer Data and are contractually bound to keep the Customer Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 We shall implement appropriate technical and organisational procedures to protect Customer Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 We shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Customer Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data transmitted, stored or otherwise processed.

4.7 The technical and organisational measures detailed in Appendix B shall be at all times adhered to as a minimum security standard. You accept and agree that the technical and organisational measures are subject to development and review and that we may use alternative suitable measures to those detailed in the attachments to this DPA provided such measures are at least equivalent to the technical and organizational measures set out in Appendix B and appropriate pursuant to our obligations in clauses 4.5 and 4.6 above

4.8 You acknowledge and agree that, in the course of providing the Services to you, it may be necessary for us to access the Customer Data to respond to any technical problems or queries and to ensure the proper working of the Cloud Service. All such access by us will be limited to those purposes defined in Appendix A.

4.9 Where Customer Data relating to an EU (or UK or Swiss) Data Subject is transferred outside of the EEA (or the UK or Switzerland) it shall be processed in accordance with the Standard Contractual Clauses unless the processing: (i) takes place in a third country or territory recognised by the EU Commission as having an adequate level of protection; or (ii) is by an organization located in a country which has other legally recognised appropriate safeguards in place.

4.10 Taking into account the nature of the processing and the information available to us, we shall assist you by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of your obligation to respond to requests for exercising the Data Subject's rights and your compliance with your data protection obligations in respect of the processing of Customer Data.

4.11 We confirm that we and/or our Affiliate(s) have appointed a data protection officer where such appointment is required by applicable data protection legislation. The appointed data protection officer may be reached at picturepark.com/terms.

5. Controller Obligations

5.1 You represent and warrant that you shall comply with the terms of the Agreement, this DPA and all applicable Data Protection Laws.

5.2 You represent and warrant that you have obtained any and all necessary permissions and authorisations necessary to permit us, our Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA.

5.3 You are responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Customer Data under this DPA and the Agreement.

5.4 All Authorised Affiliates who use the Services shall comply with your obligations set out in this DPA.

5.5 You shall implement appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. You shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

5.6 You acknowledge and agree that some instructions from you, including destruction or return of data from us, us assisting you with inspections, data protection impact assessments (DPIAs) or providing any assistance under this DPA, may result in additional fees which shall not be unreasonable. In such case, we will notify you of such fees in advance unless otherwise agreed.

6. Sub-Processors

6.1 You acknowledge and agree that: (i) Our Affiliates may be used as Sub-processors; and (ii) we and our Affiliates respectively may engage Sub-processors in connection with the provision of the Services.

6.2 We shall not authorize any Sub-processor to process Personal Data without prior notification to you as defined in 6.5.

6.3 All Sub-processors who process Customer Data in the provision of Services to you shall comply with our obligations set out in this DPA and we acknowledge and agree that we are fully responsible and liable for any Sub-processor's processing of Personal Data for the performance of its obligations under this DPA.

6.4 You agree that Sub-Processors may transfer Personal Data for the purpose of providing the Services to you in accordance with the Agreement to countries outside the European Economic Area (EEA). Where Sub-processors are located outside of the EEA, we confirm that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses with us; or (iii) have other legally recognised appropriate safeguards in place.

6.5 You authorize us to use the Sub-Processors already engaged by us on the Effective Date and we shall make available to you the current list of Sub-processors at picturepark.com/terms which shall include the identities of Sub-processors and their country of location. During the term of this DPA, we shall provide you with prior notification of at least 30 days, via email or postal mail, of any changes to the list of Sub-processor(s) who may process Customer Data before authorising any new or replacement Sub-processor(s) to process Customer Data in connection with the provision of the Services.

6.6 You may object to the use of a new or replacement Sub-processor, by notifying us promptly in writing within ten (10) Business Days after receipt of our notice. If you object to a new or replacement Sub-processor, you may terminate the Agreement or applicable Order with respect to those services which cannot be provided by us without the use of the new or replacement Sub-processor. We will refund you any prepaid fees covering the remainder of the term of the Agreement (or applicable Order) following the effective date of termination with respect to such terminated services.

7. Transfer of Data

7.1 If the Processor is located in the EEA, UK or Switzerland, ("European Territories") and processes EEA, UK or Swiss Personal Data at or from facilities in a third country, the Standard Contractual Clauses shall be incorporated by reference in this DPA. The parties agree that the Processor is the data importer and the Controller is the data exporter. Unless otherwise agreed by the parties, Appendices A and B of this DPA shall apply to the SCCs, and for the purpose of clauses 9 and 11(3) of the SCCs, the governing law will be the country in which the relevant Controller is established. Nothing in this DPA shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. Each party acknowledges that it has had the opportunity to review the Standard Contractual Clauses. In particular, the Processor acknowledges its obligations: (i) under clause 5(a) of the Standard Contractual Clauses to promptly inform the Controller of the Processor's inability to comply with the Standard Contractual Clauses; (ii) under clause 5(d)(i) of the Standard Contractual Clauses to notify the Controller of a legally binding request for disclosure by a law enforcement authority; and (iii) under clause 5(e) of the Standard Contractual Clauses to deal promptly and properly with all inquiries from the Controller relating to the processing which is the subject of the transfer.

7.2 For the avoidance of doubt, in the event that the European Commission approves a successor set of Standard Contractual Clauses ("New SCCs"), or the UK authorities issue a set of Standard Contractual Clauses ("UK SCCs"), the New SCCs and the UK SCCs shall be incorporated by reference in this DPA in place of the previously approved set of Standard Contractual clauses. In such cases, the information set out in Appendices A and B of this DPA shall be deemed to be incorporated into the appropriate sections of the New SCCs and the UK SCCs, and the Processor acknowledges the equivalent obligations in the New SCCs and UK SCCs as those set out above. To the extent that the New SCCs or UK SCCs require the inclusion of additional information not covered by Appendices A and B of this DPA, the Controller may incorporate that additional information into the New SCCs and UK SCCs by way of a written notice to the Processor.

7.3 This section applies if the Processor is established in the European Territories and engages a Sub-Processor in a third country to process EU, Swiss or UK Personal Data. In this situation, the Processor will assist the Controller and its Affiliates based in the

European Territories and/or that process Personal Data of Data Subjects in the European Territories to adduce an adequate level of protection for EU, Swiss or UK Personal Data by executing Standard Contractual Clauses with that Sub-Processor on the Controller's behalf. The Controller hereby appoint the Processor as its agent for the sole purpose of entering into such Standard Contractual Clauses on its behalf. The Processor shall provide the Controller with a copy of any Standard Contractual Clauses entered into pursuant to this section promptly on request.

8. Data Subject Access Requests

8.1 You may require correction, deletion, blocking and/or making available the Customer Data during or after termination of the Agreement. You acknowledge and agree that we will process the request, and will reasonably fulfil such request in accordance with our standard operational procedures to the extent possible.

8.2 In the event that we receive a request from a Data Subject in relation to Customer Data, we will refer the Data Subject to you unless otherwise prohibited by law. You shall reimburse us for reasonable costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request; provided you receive prior written notice regarding all such costs. In the event that we are legally required to respond to the Data Subject, you will fully cooperate with us as applicable.

9. Audit

9.1 We shall make available to you and subject to a reasonable fee all information reasonably necessary to demonstrate compliance with our processing obligations and allow for and contribute to audits and inspections.

9.2 Any audit conducted by you under this DPA shall consist of examination of our most recent reports, certificates and/or extracts prepared by us or an independent auditor bound by confidentiality provisions at least as strict as those set out in the Agreement. In the event that provision of the same is not deemed sufficient in your reasonable opinion, you may conduct a more extensive audit which will be: (i) at your expense; (ii) limited in scope to matters specific to you and agreed in advance; (iii) carried out during Swiss business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with our day-to-day business.

9.3 This clause shall not modify or limit your rights of audit in accordance with applicable law, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

10. Data Breach

10.1 We shall notify you without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Customer Data ("Data Breach").

10.2 We will promptly investigate every security breach and take reasonable measures to identify its root cause(s), mitigate its adverse effect and prevent a recurrence. As information becomes available, unless prohibited by law, we will provide you with a description of the security breach, the type of Customer Data that was the subject of the Data Breach, and other information you may reasonably request concerning the affected Customer Data.

10.3 We will take all commercially reasonable measures to secure the Customer Data, to limit the effects of any Data Breach, and to assist you in meeting your obligations under applicable law.

11. Compliance, Cooperation and Response

11.1 We will notify you promptly of any request or complaint regarding the processing of Customer Data, which adversely affects you, unless such notification is not permitted under applicable law or a relevant court order.

11.2 We may make copies of and/or retain Customer Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

11.3 We shall reasonably assist you in meeting your obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to us.

11.4 You shall notify us within a reasonable time, of any changes to Data Protection Laws, and applicable codes or regulations which may affect our contractual duties. We shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organizational measures to maintain compliance. If we are unable to accommodate reasonably necessary changes, you may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

11.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with the applicable supervisory authority in the performance of their respective obligations under this DPA and Data Protection Laws.

12. Liability

12.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

12.2 The parties agree that we shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of our Sub-processors to the same extent we would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

12.3 The parties agree that you shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of your Authorised Affiliates as if such acts, omissions or negligence had been committed by you yourself.

12.4 You shall not be entitled to recover more than once in respect of the same loss.

13. Term and Termination

13.1 The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

13.2 We shall at your choice, upon receipt of a written request received within 10 days of the effective date of termination of the Agreement, delete Personal Data according to our internal procedures or return Personal Data to you. We shall in any event within ninety (90) days of termination of the Agreement, delete all Customer Data from our systems and provide you with certificates of such deletion upon request. Excluded from this provision is Customer Data on Storage Types or Backup Options with longer retention periods for which, after termination of the Agreement, we can continue storing Customer Data for as long as twice the retention period defined for the Hosting type or Backup option plus ninety (90) days. If you make a request to have Customer Data deleted earlier than the expiry of aforementioned periods, we shall delete the Customer Data without undue delay, for a reasonable charge unless prohibited from doing so by applicable law.

14. General

14.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

14.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

14.3 Subject to any provision of the Standard Contractual Clauses to the contrary, this DPA shall be governed by the law applicable to the terms of the Agreement. The courts that shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA shall be the same as those set out in the terms of the Agreement.

14.4 The provisions of this DPA shall survive the termination of other relevant existing Agreement(s) and continue as long as we have possession of your Personal Data.

14.5 Any notices under this DPA shall be in writing, sent via email to the email addresses as provided in the Order Documents with a copy sent via email to legal@picturepark.com.

PICTUREPARK

Appendix A:
Overview of data processing activities to be performed by us.

1. Controller

You as the Data Controller will use the Services or grant users the right to access the Cloud Service in accordance with the terms of the Agreement for transfer of Customer Data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

2. Processor

We as the Data Processor receive data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

3. Data Subjects

You acknowledge and agree that the categories of Data subjects that use and might process Customer Data via the Services are solely determined by you and your User's use of the Cloud Service. Notwithstanding the foregoing, the Customer Data processed usually concerns the following categories of Data Subjects:

- Employees, freelancers and contractors of you.
- Users, Authorised Affiliates and other participants.
- Partners, suppliers or service providers of you
- Customers of you or your media contacts.
- Any individual to whom you have granted the right to access the Services in accordance with the terms of the Agreement.
- Other individuals to the extent identifiable through their use or registration with the Cloud Service, or through content of files or metadata processed with the Services.

4. Categories of Customer Data

The categories of Customer Data processed is solely determined by you and your Users use of the Services but when using the Cloud Service as a registered user which may include the User's full name, email, address, password and IP address. Customer Data might be stored in database records, metadata and files on file systems which identify or may reasonably be used to identify, Data Subjects.

When using the Cloud Service, you agree and acknowledge that you and your Users will abide by the Acceptable Use Policy (AUP) and that Customer Data including Personal Data is only processed via the Cloud Service with the prior written consent of the Data Subject.

5. Special categories of Personal Data

We do not require any special categories of Personal Data for using the Services such as, for example only, data of minors. Your and your User's use of the Services solely determine if and which special categories of Personal Data are stored and processed.

6. Processing operations

The Customer Data processed will be subject to the following basic processing activities:

Customer Data will be processed to the extent necessary to provide the Services in accordance with both the Agreement and your instructions. We process Customer Data only on behalf of you, the Data Controller.

Processing operations include, but are not limited to:

- Provision of the Cloud Service via our hosting infrastructure.
- Auditing use of the Cloud Service for compliance with the Agreement or applicable law.
- Analysing the usage of the Cloud Service and Customer Data for the purpose of protecting it against threats or for improving the Cloud Service.
- Provision of Technical support, issue diagnosis and Defect resolution to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Cloud Service and specifically in answer to Support queries of you or your users.
- Informing users about changes, issues or maintenance work related to the Cloud Service.
- Complying with your requests for Professional Services or auditing that involve accessing and processing Customer Data.
- Fulfilling any other obligation set out in the Agreement.

All these operations relate to all categories and aspects of Customer Data processed.

PICTUREPARK

Appendix B:
Technical and Organisational Security Measures

The following descriptions provide an overview of the technical and organisational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available. It's acknowledged and agreed that the technical and organisational measures described therein and in our internal IT & Security Policies will be updated and amended from time to time, at our sole discretion. Notwithstanding the foregoing, the technical and organisational measures will not fall short of those measures described in our IT Security Policy in any material, detrimental way.

1. Hosting infrastructure

We utilise third party Hosting infrastructure for the Cloud Service in form of data centres and Infrastructure-as-a-Service (IaaS) with organizations that maintain current ISO 27001 certifications, and optionally: ISO 27017 and/or ISO 27018 certifications.

Except as otherwise specified for the Services or parts thereof, we will not utilise third party data centres or IaaS providers for hosting our Cloud Service that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Excluded from the forgoing is our internal IT infrastructure used for Services such as backups, POC, staging, testing or project implementation, and for which substantially similar requirements apply without requiring attestation of such certifications.

2. Physical Access Control.

Technical or organisational measures regarding access control, especially regarding legitimation of authorised persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Customer Data.

We employ measures designed to prevent unauthorized persons from gaining access to data processing systems that we use for the Services.

For our Cloud Service the constructional and substantive security standards comply with the security requirements for data centres that maintain at least ISO 27001 certifications, and optionally: ISO 27017 or/and ISO 27018 certifications.

Excluded from the forgoing is our internal IT infrastructure used for Services such as backups, POC, staging, testing or project implementation, and for which substantially similar requirements apply without requiring attestation of such certifications.

3. System Access Control.

Technical and organisational measures regarding the user identification and authentication:

The aim of the system access control is to prevent unauthorised use of data processing systems used for the processing of Customer Data.

The following may, among other controls, be applied depending upon the particular Services ordered: authentication via passwords and/or two-factor authentication, documented authorization and change management processes, and logging of access on several levels.

For all our Services: (i) log-ins to data storage or processing systems are logged; (ii) logical access to the data storage and processing centers is restricted and protected by VLAN/VPN; and (iii) centralized logging and alerting, and firewalls are used.

4. Data Access Control.

Technical and organisational measures regarding the authorisation concept, data access rights and monitoring and recording of the same:

Measures regarding data access control are targeted on the basis that only such data can be accessed for which an access authorisation exists and that data cannot be read, copied, changed or deleted in an unauthorised manner during the processing and after the saving of such data.

Customer Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept.

5. Transmission Control.

Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Customer Data on data media (manually or electronically).

Transmission control is implemented so that Customer Data cannot be read, copied, changed or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which particular recipients a transfer of Customer Data is intended.

Except as otherwise specified for the Services or parts thereof, transfers of data outside the Cloud Service environment and our internal IT infrastructure used for Services such as backups, POC, staging, testing or project implementation are encrypted and/or stored on encrypted media. Backup media such as tapes used for the Suisse Safe Backup Option are always encrypted.

The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. You are responsible for the results of your decision to use unencrypted communications or transmissions when exchanging data with us through such email or messaging services, or when using part of the Cloud Service that rely on sending content through such email or messaging services.

The transfer of Customer Data to a third party (e.g. sub-processors) is only made if a corresponding agreement exists, and only for the specific purposes. If Customer Data is transferred to companies located outside the EEA (or the UK or Switzerland), we provide that an adequate level of data protection exists at the target location or organisation in accordance with our obligations of this DPA, e.g. by employing contracts based on the Standard Contractual Clauses.

Customer Data used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.

6. Data Entry Control.

Technical and organisational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review:

Data Entry Controls are implemented so that a retroactive review is enabled.

System inputs are recorded in the form of log files and database records therefore it is possible to review retroactively whether and by whom Customer Data was entered, altered or deleted.

7. Data Backup and Availability Control.

Technical and organisational measures regarding data backup (physical/logical):

Data backup and availability controls are implemented to protect Customer Data against accidental destruction and loss.

Backups for our Cloud Services are taken on a regular basis where you have chosen a corresponding Hosting type or Backup option as defined in the Agreement. It is your sole responsibility to select such corresponding options providing you with adequate data backup and availability control.

Backup media transferred outside of the Hosting infrastructure of the Cloud Service and our internal IT infrastructure used for Services such as backups, POC, staging, testing or project implementation is always encrypted except we are instructed otherwise by you for which you are then responsible.

8. Data Processing Control

Technical and organisational measures to differentiate between the competences of the data controller and the data processor:

The aim of the data processing control is to provide that Customer Data is processed by a commissioned data processor in accordance with the Instructions of the data controller.

Details regarding data processing control are set forth in the Agreement and DPA.

9. Data Segregation.

Technical and organisational measures regarding purposes of collection and separated processing:

Customer Data from our different customer environments is logically segregated on our systems or those of Sub-processors by technical or organisational means.

Employees are instructed to collect, process and use Customer Data only as per the definitions of our IT & Security Policies and for the purposes of their duties only (e.g. provision of Professional Services), and to delete such Customer Data if no longer required for the purpose of the delivery of Services or as required by applicable law.

Customer Data processed via our Cloud Service is stored in a way that logically separates it from other customer data.

Appendix C:
Standard Contractual Clauses

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

……, (the data **"exporter"**)

and

……„(the data **"importer"**)

each a "**party**"; together "**the parties**",

HAVE AGREED on the following Standard Contractual Clauses (the "**Standard Contractual Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix A of the DPA.

Clause 1

Definitions

For the purposes of the Standard Contractual Clauses all terms used in capitals shall have the meaning given to them in the DPA unless defined otherwise below:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(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 Standard Contractual Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 Standard Contractual 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 Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 Appendix A of the DPA which forms an integral part of the Standard Contractual Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 subprocessor 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 subprocessor shall be limited to its own processing operations under the Standard Contractual 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 Standard Contractual Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in the Security Policy;

(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, unauthorised 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 providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority 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 Standard Contractual Clauses, with the exception of the Security Policy, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Standard Contractual Clauses, unless the Standard Contractual Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer[2]

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 Standard Contractual 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 Standard Contractual 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 organisational security measures specified in the Security Policy before processing the personal 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 unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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 supervisory authority 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 Standard Contractual 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 supervisory authority;

(g) to make available to the data subject upon request a copy of the Standard Contractual Clauses, or any existing contract for subprocessing, unless the Standard Contractual Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of the Security Policy 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor agreement it concludes under the Standard Contractual 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Standard Contractual 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 subprocessor shall be limited to its own processing operations under the Standard Contractual 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 Standard Contractual 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 supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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 supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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 Standard Contractual Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Standard Contractual Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Standard Contractual Clauses.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Standard Contractual Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Standard Contractual Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Standard Contractual Clauses[3]. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Standard Contractual Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Standard Contractual 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 data exporter's data protection supervisory authority.

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 subprocessor 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 subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Miscellaneous

1. These Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Standard Contractual Clauses are entered into.