PICTUREPARK

Data Processing Agreement (DPA)

Last changed: 28 February 2022

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 and B;
“Effective Date”	means the 27th of December 2022 or the date on which you entered into the Agreement, if on or after the 27th of September 2021 or the date as mutually defined in the Order Document or required by law;
“EEA”	means the European Economic Area;
“EU GDPR”	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
“Internal IT Infrastructure”	means our internal IT infrastructure which is used for our corporate use as well as for processing Customer Data for the purpose of creating and storing backups of select Customer Data, providing Professional Services and Technical Support, or hosting the Cloud Service for Proof-of-concept (POC) engagements with clients or prospects, customer staging, or product development purposes;
“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;
“Restricted Transfer”	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

	iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
"Services"	means our Cloud Service, Technical Support or any Professional Services provided by us to You and Authorised Affiliates;
"SCCs"	Means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN/, ("**EU SCCs**"); and (ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR published at https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/, ("**UK SCCs**"); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; ("**Swiss SCCs**");
"Sub-Processor"	means any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller;
"Supervisory Authority"	means a governmental or government chartered regulatory body having binding legal authority over a party;
"Swiss FADP"	means the Swiss Federal Act on Data Protection (Swiss FADP) as published in AS 1993 1945 and any newer corresponding act or regulation (especially the "new FADP 2022";
"UK GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 as implemented into UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018.

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 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.

4.10 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 6.4.

6.3 All Sub-processors who process Customer Data in the provision of Services to you shall: (i) comply with our obligations set out in this DPA; (ii) be appointed under a written contract containing materially the same as our obligations in this DPA enforceable by us; and (iii) 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 authorize us to use the Sub-Processors included in the list of Sub-processors at picturepark.com/terms to process Customer Data. 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-processors who may process Customer Data before authorising any new or replacement Sub-processor to process Customer Data in connection with the provision of the Services.

6.5 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.

6.6 You agree that we and our Sub-Processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to you in accordance with the Agreement. We confirm that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have entered the applicable SCCs with us; or (iii) have other legally recognised appropriate safeguards in place.

7. Restricted Transfers

7.1 The parties agree that, when the transfer of Customer Data from you to us or from us to a Sub-processor is a Restricted Transfer, it shall be subject to the applicable SCCs.

7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

(i) Module Two (Controller to Processor) shall apply where the You are a Controller of Customer Data and we are processing Customer Data;

(ii) Module Three (Processor to Processor) shall apply where we are a Processor of Customer Data and we use a Sub-processor to process the Customer Data;

(iii) In Clause 7 of the EU SCCs, the optional docking clause will not apply;

(iv) In Clause 9 of the EU SCCs Option 2 applies, and the time period for giving notice of Sub-processor changes shall be 30 days;

(v) In Clause 11 of the EU SCCs, the optional clause/language shall not apply;

(vi) In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Austrian law;

(vii) In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Austria;

(viii) Annex I of the EU SCCs shall be deemed completed with the information set out in Appendix A of this DPA;

(ix) Annex II of the EU SCCs shall be deemed completed with the information set out in Appendix B of this DPA;

7.3 The parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the Swiss FADP applies to any Restricted Transfer:

(i) The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the Swiss FADP;

(ii) Restricted Transfers subject to both the Swiss FADP and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Appendix A of this DPA;

(iii) The term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

(iv) Where Restricted Transfers are exclusively subject to the Swiss FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the Swiss FADP;

(v) Where Restricted Transfers are subject to both the Swiss FADP and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the Swiss FADP insofar as the Restricted Transfers are subject to the Swiss FADP;

(vi) The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the revised Swiss FADP.

7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:

(i) Appendix 1 of the UK SCCs shall be deemed completed with the information set out in Appendix A of this DPA; and

(ii) Appendix 2 of the UK SCCs shall be deemed completed with the information set out in Appendix B of this DPA.

7.5 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.

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. Personal 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 ("Personal 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 Personal 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 Personal 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.

14. Deletion and Return of Personal Data

14.1 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.

15. General

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

15.2 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.

15.3 Subject to any provision of the SCCs 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.

15.4 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.

15.5 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:
List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority.

MODULE TWO: CONTROLLER TO PROCESSOR

A. LIST OF PARTIES

The Controller means **you** with name and address at: As set out for you in the Agreement or the Order Documents.	
Contact person's name, position and contact details:	As provided by you, the Controller, in your account of the Cloud Service and/or Order Documents, used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services.
Signature and date:	By entering into the Agreement, you are deemed to have signed the SCCs incorporated into this DPA and including their Annexes, as of the effective date of the Agreement.
Role:	Data Exporter.
Name of Representative (if applicable):	Any UK or EU representative named in your privacy policy.

The Processor means **us** (Picturepark) with address at: Vision Information Transaction AG (known as "Picturepark") Industriestrasse 25 CH-5033 Buchs (AG), Switzerland	
Contact person's name, position and contact details:	Picturepark DPO as published online on https://picturepark.com/terms/dpo/.
Activities relevant to the data transferred under the SCCs:	The provision of cloud computing solutions to you under which the Processor processes Personal Data upon your instructions in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Processor is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes, as of the effective date of the Agreement.
Role:	Data Importer

Name of Representative (if applicable):	See https://prighter.com/q/15848945763 for our current EU GDPR or UK GDPR representatives: EU GDPR representative: PrighterGDPR-Rep by Maetzler Rechtsanwalts GmbH & Co KG Schellinggasse 3/10 1010 Vienna, Austria https://prighter.com, support@prighter.com Please add the following subject to all correspondence: ID-15848945763 UK GDPR representative: PrighterUK-Rep by Prighter Ltd 20 Mortlake Mortlake High Street London, SW14 8JN, United Kingdom https://prighter.com, support@prighter.com Please add the following subject to all correspondence: ID-15848945763

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects:	Your authorised users of the Services, including but not limited to: • Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons). • Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement. • Prospects, customers, clients, business partners and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. • Employees or contact persons of Controller's prospects, customers, clients, business partners and vendors. • Suppliers and service providers of the Controller. • Other individuals to the extent identifiable in the context of data processed via the Services, via emails or their attachments, in archiving content or other files, databases or similar.
Categories of Personal Data:	You as the Controller through your authorised users may submit Personal Data to the Services, the extent of which is determined and controlled by the Controller. The Personal Data includes but is not limited to: • Personal details of users of the Services including names, role, function, email addresses, username, account number, unique identifiers. • Personal Data derived from a user's use of the Services such as statistical records, business intelligence information, IP addresses, names of Internet providers, geolocation data, web browser information, URL, URL clickstream. • Images, videos, documents, sound recordings and any other files that contain Personal Data as content or within their metadata. • Metadata, annotations or other information and any data created, stored, managed or exchanged via the Services that may contain Personal Data. • Email and messaging content which identifies or may reasonably be used to identify, Data Subjects. • Meta data related to email or data transfer activities through the Services including recipient, sender, date, time, subject data, which may include Personal Data. • Data you entered for searching or filtering content which might contain Personal Data. • Information offered by users as part of support queries, and data recorded, stored and processed when engaging with our support.

	• Other data added or managed by the Controller from time to time for processing using the Services.
Sensitive Data:	The Processor does not require any special categories of Personal Data for using the Services. You and your authorised user's use of the Services solely determine if and which special categories of Personal Data are stored and processed.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	The principle nature of the processing is to provide you as the Controller the Cloud Service and other Services. Processing operations include but are not limited to: • Provision of the Cloud Service via our hosting infrastructure. • Auditing the usage of the Service for compliance with the Agreement or applicable law. • Analysing the usage of the Service and Customer Data for the purpose of protecting it against threats or for improving the 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 Service and specifically in answer to Support Queries of you or your users. • Informing users about changes, issues or maintenance work related to the 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.
Purpose(s) of the data transfer and further processing:	Customer Data including Personal Data is transferred to sub-processors who need to process some of the data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for the duration of the Agreement, subject to clause 14 of the DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list accessed via https://picturepark.com/terms sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	• Where the EU GDPR applies, the Austrian Data Protection Authority. • Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). • Where the Swiss FADP applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

MODULE THREE: PROCESSOR TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is us (Picturepark).

The Data Importers: are the Sub-processors named in the Sub-processor list which contains the name, address, contact details and activities relevant to the data transferred to each Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

The Sub-processor list includes the information about the processing and transfers of the Personal Data, for each Data Importer:

- categories of Data Subjects
- categories of Personal Data
- the nature of the processing
- the purposes of the processing

Personal Data is processed by each Data Importer:

- on a continuous basis
- to the extent necessary to provide the Services in accordance with the Agreement and the Data Exporter's instructions.
- for the duration of the Agreement and subject to clause 14 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority of the Data Exporter shall be:

- Where the EU GDPR applies, the Austrian Data Protection Authority.
- Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO).
- Where the Swiss FADP applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

Appendix B:
Technical and Organisational Security Measures

(Including Technical and Organizational Measures to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by us to ensure an appropriate level of security, considering the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Where applicable this Exhibit B will serve as Annex II to the SCCs.

Measure	**Description**
Measures of pseudonymisation and encryption of Personal Data	For the purpose of transfer control, encryption technologies are used. The suitability of an encryption technology is measured against the protective purpose. Except as otherwise specified for the Services or parts thereof, Customer Data in transit outside the secured networks of the Cloud Service and our Internal IT Infrastructure or any Customer Data in transit that qualifies as Restricted Transfer, is protected by using Transport Layer Security ("TLS"). Except as otherwise specified for the Services or parts thereof, if Customer Data at rest is stored outside the secured infrastructure of the Cloud Service and our Internal IT infrastructure or any Customer Data at rest that qualifies as Restricted Transfer, is protected by using AES256 bit encryption, or encryption that provides substantially similar protection. Backup media such as tapes used for the Suisse Safe Backup Option or backups of our systems in use for corporate or operations purposes are always encrypted using AES128 bit encryption and continuously overwritten according our backup rotation and retention schedules. Note that where you have selected "Europe" or "Switzerland" as the Region, or where you have selected the Suisse Safe Backup Option, Customer Data at rest will solely be stored in the EEA (including Switzerland) or Switzerland as per the definitions in the Agreement. Company laptops are encrypted using AES-256 encryption or similar, for use of other devices that access Customer Data, our General IT & Security Policies applies. Access to our Internal IT infrastructure requires use of secure protocols such as HTTPS with SSL/TLS, VPN tunneling, or similar.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	To maintain confidentiality and integrity, and where deemed appropriate to protect Customer Data based on risk, industry standard encryption technology is applied to the Customer Data itself or the storage media that contains Customer Data. Access to Customer Data necessary for the performance of the particular task is provided in accordance to the "least privilege" and "need-to-know" principles, and requires secure authentication using individual user accounts and strong passwords which are always encrypted. Access to systems is restricted by security groups and access-control lists. Accounts are locked after multiple failed access attempts. Whenever remote access to any of our system is used for the Cloud Service or our Internal Infrastructure, we use VPN tunnelling or https (SSL/TLS) secured connections and multi-factor authentication. Where reasonably possible, access is granted temporarily only and access to systems and information is logged. Availability and resilience of Personal and Customer Data is maintained by using redundant infrastructure, mirroring Customer Data or performing periodic backups of Customer Data which might depend on the Storage Types and Backup Options that you selected for the Cloud Service. Additionally, we have disaster recovery and

	business continuity plans in place in order to mitigate the adverse effects of disasters. Systems for production use of our Cloud Service are physically separated from our Internal IT Infrastructure.
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident	We maintain redundancy as appropriate throughout our IT infrastructure in order to minimize the lack of availability to or loss of Customer Data. Where you have selected corresponding Storage Types, Customer Data is stored in one or multiple data centres for mitigating destruction or loss of Customer Data, and for restoring the Services as quickly as possible, as defined in our Agreement. Where you have selected corresponding Backup Options, Customer Data might be stored in additional data centres using save guards such as encrypted storage on offline backup tapes in place as defined in our Agreement. Backups are maintained in accordance with our backup procedures. We maintain a disaster recovery and business continuity plans which are verified periodically and at least once per calendar year.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	We periodically conduct security assessments as well as vulnerability and penetration tests on our infrastructure used for providing the Services. Wherever reasonably possible and for early on detection of any security issues, we automate the continuous testing and review of rest results in such way that it is integrated in development and release of new versions of our Cloud Service. Our test systems are logically and/or physically separated from our production systems and environments. We periodically review and improve our security policies.
Measures for user identification and authorisation	Access to Customer Data necessary for the performance of the particular task is provided in accordance to the “least privilege” and "need-to-know" principles, and requires secure authentication using individual user accounts and strong passwords which are always encrypted and enforced, and which need to be changed periodically or triggered by events such as the change of role of or the employment termination with employees. Access to systems is restricted by security groups and access-control lists. Accounts are locked after multiple failed access attempts. Remote access to the data processing systems of the Cloud Service and our Internal IT infrastructure is only possible through a secure VPN tunnel or via https (SSL/TLS) secured connections, with multi-factor authentication in place. Network-specific firewalls are in place to protect our different IT infrastructures used for the provisioning of the Services including our Internal IT Infrastructure. Authorization requests and provisioning as well as select user activities are logged.
Measures for the protection of data during transmission	Except as otherwise specified for the Services or parts thereof, Customer Data in transit outside the secured networks of the Cloud Service and our Internal IT Infrastructure or any Customer Data in transit that qualifies as Restricted Transfer, is protected by using Transport Layer Security (“TLS”). Remote access to the data processing systems of the Cloud Service and our Internal IT infrastructure is only possible through a secure VPN tunnel or via https (SSL/TLS) secured connections, with multi-factor authentication in place.
Measures for the protection of data during storage	Except as otherwise specified for the Services or parts thereof, if Customer Data at rest is stored outside the secured infrastructure of the Cloud Service and our Internal IT infrastructure or any Customer Data at rest that qualifies as Restricted Transfer, is protected by using AES256 bit encryption, or encryption that provides substantially similar protection. Backup media such as tapes used for the Suisse Safe Backup Option or backups of our systems in use for corporate or operations purposes are always encrypted using AES128 bit encryption and continuously overwritten according our backup rotation and retention schedules.
Measures for ensuring physical security of locations at which Personal Data are processed	Due to their respective security requirements of our corporate premises and the data centre of our Internal IT infrastructure are subdivided into different security zones with different access authorisations in use. CCTV monitoring is in place 24/7.

	The data centres used for providing our Cloud Service comply with the constructional and substantive security standards and requirements for data centres that maintain at least ISO 27001 certifications. Excluded from the forgoing is our Internal IT infrastructure for which substantially similar requirements apply without requiring attestation of such certifications.
Measures for ensuring events logging	Various security relevant events of the systems and infrastructure for providing our Services are logged, monitored and analysed as required. Access onto systems and networks require users to authenticate and every access attempt, successful or unsuccessful, is logged to a centralised service, or on the corresponding system. Logs are usually retained for multiple month or a period as deemed appropriate for the concerned service based on its data processing classification and in order to meet retroactive security auditing as well as data protection needs.
Measures for ensuring system configuration, including default configuration	Wherever possible, our system configuration is based on our internal templates, images or containers that use industry best practise configurations and application security systems that enhance the operating system. Prior to applying configurations or code changes onto production systems, these configurations or code undergo strict quality control processes on physically or logically separated QA (testing or staging) systems. Excluded from the foregoing are emergencies for which we reasonably decide to apply changes immediately for mitigating potential or effective adverse effects of security incidents.
Measures for internal IT and IT security governance and management	Employees are instructed to collect, process and use Customer Data only within the framework and for the purposes of their duties e.g. providing Technical Support based on Support Queries or select Professional Services. All Customer Data must be processed according our General IT & Security Policies or other documented security and data protection instructions. Our IT and security policies and processes are periodically reviewed and improved in order to meet industry best practise and relevant standards.
Measures for certification/assurance of processes and products	We only utilise third party Infrastructure as a Service (“IaaS”) or Platform-as-a Service (“PaaS”) providers for providing our Cloud Service with data centres that maintain current ISO 27001 certifications, and optionally: SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports, or that have other substantially similar or equivalent certifications and/or attestations. Upon your written request (no more than once in any 12-month period), we shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to you as the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties Excluded from attestation of certification is our internal IT infrastructure for which similar requirements apply without requiring attestation of such certifications. Our IT and security policies as well as our software development processes are periodically reviewed and improved in order to meet industry best practises and relevant standards.
Measures for ensuring data minimisation	If Customer Data is no longer required for the purposes for which it was processed, it is deleted as per the retention policies in this DPA and our Agreement with you. Wherever possible with each deletion, the Customer Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental or possible intentional deletions by a third party. Data collection is limited to the purposes of processing (or the data that the customer chooses to provide). Internal security measures are in place to provide only the minimum amount of access necessary to perform required functions. We restrict access to Customer Data to the parties involved in the processing in accordance with the “need to know” principle and according differentiated access profiles.
Measures for ensuring data quality	All of the Customer Data processed is provided by you, the Controller. We do not assess the quality of the Customer Data provided by you. We provide built-in features

	in the Cloud Service to help you understand and validate the quality of the Customer Data that your stored. Our Cloud Service is designed to ensure data integrity with multiple application and system-level checks in place. Our continuous testing process ensures that the Cloud Service is working as designed before being deployed in our production environment.
Measures for ensuring limited data retention	We use a data classification scheme for all Customer Data that we store which also defines default data retention times. When Customer Data is deleted then it will be permanently removed from our active systems and databases with a certain delay after being locked in the first instance, as appropriate. Customer Data might be retained in backups or other safeguard storages until they are replaced by more recent backups or deleted, as per the retention periods defined in the Agreement and this DPA.
Measures for ensuring accountability	We internally review our IT & security policies as needed and at least once per year to ensure they are still relevant, according industry best practises, and that they are being followed. All employees including contractors that handle Customer Data must acknowledge our Internal IT &Security Policies. Disciplinary or legal sanctions are in place for employees that do not adhere to these policies. Employees are re-trained at least once per year on our IT & Security Policies or other applicable policies in place. Data protection impact assessments are part of new data processing initiatives such as when evaluating new sub-processors (or re-evaluating existing sub-processors as required from time to time) and substantially changing data processing processes and systems.
Measures for allowing data portability and ensuring erasure	The Cloud Service has built-in features that allow you to export and delete Customer Data. We also provide an API which can be accessed by the users of an account with CRUD actions on all main entity types of Customer Data. Additionally, we provide you Professional Services for standardised exports of Customer Data at predefined terms (no “lock-in”), as defined in our Agreement. When your use of the Cloud Service becomes terminated, we erase Customer Data in compliance with our retention policies as defined in the Agreement and DPA.
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter).	In general, the transfer of Customer Data to a third party is only made if a corresponding agreement exists, and only for the specific purposes. If Customer Data is transferred outside the EEA, we ensure that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements and other applicable regulations, e.g. by employing contracts based on the EU SCCs.