PICTUREPARK

# Data Processing Agreement (DPA)

Last changed: 20 December 2019

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; |
| **“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 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, 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. |
| **“DPA”** | means this data processing agreement together with its Appendices A and B; |
| **“Effective Date”** | means the 25th of May 2018 or the date on which you entered into the Agreement, if after the 25th of May 2018, or as mutually defined in the Order Document; |
| **“Personal Data”** | shall have the same meaning as in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, 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. |
| **“Processor”** | means us; |
| **“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 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. |

## 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.

## 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 and shall take steps to ensure that any natural person acting under the authority of us who has access to Customer Data does not process the Customer Data except on instructions from you.

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.

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 Controller 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 it shall be processed by an entity: (i) located in a third country or territory recognised by the EU Commission as having an adequate level of protection; or (ii) that is subject to Standard Contractual Clauses; or (iii) that has other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

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 www.picturepark.com/terms/dpo.

## 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 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.

5.6 You 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.

5.7 You shall take steps to ensure that any natural person acting under your authority who has access to Customer Data does not process the Customer Data except on your instructions.

5.8 You may require correction, deletion, blocking and/or making available the Customer Data during or after termination of the Agreement. We will process the request to the extent it is lawful, and will reasonably fulfil such request in accordance with our standard operational procedures to the extent possible.

5.9 You acknowledge and agree that some instructions from you, including destruction or return of data from us, may result in additional fees. 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 All Sub-processors who process Customer Data in the provision of Services to you shall comply with our obligations set out in this DPA.

6.3 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, such as the EU-US Privacy Shield or Binding Corporate Rules.

6.4 We shall make available to you the current list of Sub-processors at www.picturepark.com/terms/dpa-subprocessors 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, 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.

6.5 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, and that objection is not unreasonable, 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. Liability

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

7.2 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.

7.3 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.

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

## 8. Audit

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

8.2 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.

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

## 9. Notification of Data Breach

9.1 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**").

9.2 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.

9.3 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.

## 10. Compliance, Cooperation and Response

10.1 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 all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that we are legally required to respond to the Data Subject, you will fully cooperate with us as applicable.

10.2 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.

10.3 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.

10.4 The parties acknowledge that it is the duty of you to notify us within a reasonable time, of any changes to applicable data protection laws, 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. If the parties agree that amendments are required, but we are unable to accommodate the 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.

10.5 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.

## 11. Term and Termination

11.1 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.

11.2 We shall within forty-five (45) 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 forty-five (45) days. If you make a request to have Customer Data deleted earlier than the expiry of the extended storage period, we shall delete the Customer Data without undue delay, for a charge unless prohibited from doing so by applicable law.

## 12. General

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

12.2 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.

12.3 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.

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 this will include at the minimum 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 have to strictly 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.

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

## 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.
- Finding, analysing and protecting the Cloud Service and Customer Data or users against threats.
- 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 your Support query.
- 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 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/or SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. 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.

## 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 SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. Excluded from the forgoing is the Suisse Safe Backup Option for which substantially similar requirements apply without requiring attestation of such certifications. For the Suisse Safe Backup Option all data is encrypted at rest and during transfer.

## 3. System Access Control.

Technical and organisational measures regarding the user ID 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 processes, documented 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 Service or parts thereof, transfers of data outside the Cloud Service environment are encrypted and/or stored on encrypted media.

The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. You are solely responsible for the results of your decision to use unencrypted communications or transmissions when exchanging data with us 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 contract exists, and only for the specific purposes. If Customer Data is transferred to companies located outside the EEA, 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 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 Policy and for the purposes of their duties (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 mandatory law.

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