



## INTELLECT SELECT

### Data Processing Agreement

between

Client Name

Client Address

("Data Controller") and

**Intellect Select limited**

Company reg. no. 11362885

71-75 Shelton Street, Covent Garden,

London, WC2h 9JQ, United Kingdom

("Data Processor")

(together referred to as the "Parties" or individually as a "Party")

## Contents

1. Preamble.....	3
2. The rights and obligations of the Data Controller.....	4
3. The Data Processor acts according to instructions.....	4
4. Confidentiality.....	4
5. Security of processing.....	5
6. Use of Sub-processors.....	5
7. Transfer of data to third countries or international organizations.....	6
8. Assistance to the Data Controller.....	7
9. Notification of personal data breach.....	8
10. Erasure and return of data.....	9
11. Audit and inspection.....	9
12. Commencement and termination.....	9
13. Data Controller and Data Processor contacts/contact points.....	10
Appendix A: Information about the processing.....	11
Appendix B Authorized Sub-processors.....	12
Appendix C Instruction pertaining to the use of personal data.....	13
Appendix D Obligations of the Data Controller.....	15
Appendix E Limitation of liability.....	15

## 1. Preamble

1. The Parties have agreed on the following contractual terms (“Terms”) to ensure compliance with Article 28 (3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (“GDPR”) and to ensure the protection of the rights of the data subject (“Data Subject”).
2. The Terms in this data processing agreement (“DPA”) sets out the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller with reference to the Parties Master Agreement “XX” entered and signed “XX” concerning the Data Controller’s use of the Data Processor’s products and services (“Services”). The Data Processor will process personal data on behalf of the Data Controller in accordance with the Terms herein.
3. The Terms takes priority over any similar provisions contained in other agreements between the Parties.
4. Five appendices are attached to the Terms and constitutes an integral part of the Terms and this DPA.
5. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of Data Subject and duration of the processing.
6. Appendix B contains the Data Controller’s conditions for the Data Processor’s use of Sub-processors and a reference list of Sub-processors authorized by the Data Controller.
7. Appendix C contains the Data Controller’s instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the Data Processor, and how audits of the Data Processor and any Sub-processors are to be performed.
8. Appendix D contains information pertaining to obligations of the Data Controller.
9. Appendix E regulates the Parties limitation on liability under this DPA.
10. The Terms along with appendices must be retained in writing, including electronically, by both Parties.
11. The Terms does not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

## 2. The rights and obligations of the Data Controller

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with Article 2 of the GDPR, the applicable EU or EEA Member States data protection provisions and the Terms.
2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The Data Controller is responsible, among other, for ensuring that the processing of personal data, which the Data Processor is instructed to perform is lawful in accordance with Article 6 of the GDPR.

## 3. The Data Processor acts according to instructions

1. The Data Processor process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the processor is subject. Instructions of the Data Controller and the Data Processor's authorization of processing are specified in appendices A and C.
2. If the processing of Personal Data by the Data Processor occurs as a consequence of a legal obligation of the Provider under laws or regulations applicable to the Provider, the Provider has the obligation to notify the Data Controller with respect to such legal obligation at least three (3) business days before the processing starts, unless such laws and regulations prohibit such notification;
3. When processing Personal Data under Art. 2. above, the Data Processor shall restrict processing to the minimum extent necessary and avoid processing or disclosing Personal Data which is not required by applicable laws and regulations or the competent supervisory authorities. The Data Processor shall comply with the Data Controller's reasonable instructions with regards to the processing or disclosure of Personal Data
4. The Data Processor must immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, such instructions must always be documented and kept in writing, including electronically, in connection with the Terms.

## 4. Confidentiality

1. The Data Processor should only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who are required access to the personal data in order to fulfil the contractual obligations of the Data Processor to the Data Controller and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and limited to need to know basis.

2. The Data Processor should at the request of the Data Controller demonstrate that the concerned persons under the Data Processor's authority are subject to the abovementioned confidentiality.

## 5. Security of processing

1. Article 32 of the GDPR stipulates that, 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, the Data Controller and Data Processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- a. Pseudonymization and encryption of personal data;
  - b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
2. According to Article 32 GDPR, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks.
  3. The Data Processor's implemented technical and organizational measures subject to the processing is specified in Appendix C of this DPA and the Data Processor ensures that it will under all circumstances, as minimum, implement the level of security as specified in Appendix C.
  4. If subsequently – in the assessment of the Data Controller – mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall specify these additional measures to be implemented in Appendix C.

## 6. Use of Sub-processors

1. The Data Processor must meet the requirements specified in Article 28(2) and (4) of the GDPR in order to engage another processor ("Sub-processor").
2. The Data Processor can therefore not engage another Sub-processor for the fulfilment of the Terms without the prior general written authorization of the Data Controller.

3. The Data Controller gives the Data Processor its general prior authorization for the engagement of Sub-processors. The Data Processors' notification to the Data Controller of any intended changes concerning the addition or replacement of Sub-processors, as well as the Data Controllers' right to object to the prior engagement of the concerned Sub-processor(s) are regulated in Appendix B.
4. The list of Sub-processors already engaged by the Data Processor and authorized by the Data Controller can be found in Appendix B.
5. Where the Data Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the Terms shall be imposed on that Sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Terms and the GDPR.

The Data Processor is therefore responsible for requiring that its Sub-processors at least comply with the obligations to which the Data Processor is subject pursuant to the Terms and the GDPR.

The Data Processor shall only select Sub-processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner so that the processing will meet the requirements of this Agreement, Data Protection Regulations and ensure the protection of the rights of the Data Subject

6. A copy of such a Sub-processor agreement and subsequent amendments must – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the Terms are imposed on the Sub-processor. Terms on business related issues that do not affect the legal data protection content of the Sub-processor agreement, is not required to be submitted to the Data Controller.
7. The Controller should – in the event of bankruptcy of the Data Processor – have the opportunity to be a third-Party beneficiary subject to the Sub-processor agreement, and have the right to enforce the agreement against the Sub-processor engaged by the Data Processor, e.g. to instruct the Sub-processor to delete or return the personal data.
8. If a Sub-processor does not fulfil its data protection obligations, the Data Processor remains fully liable towards the Data Controller as regards the fulfilment of the obligations of the Sub-processor. This does not affect the rights of the Data Subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the Sub-processor.

## 7. Transfer of data to third countries or international organizations

1. Any transfer of personal data to third countries or international organizations by the Data

Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organizations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law to which the Data Processor is subject, the Data Processor should inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
3. Without documented instructions or approval from the Data Controller, the Data Processor cannot within the framework of the Terms:
  - a. transfer personal data to a Data Controller or a Data Processor in a third country or in an international organization
  - b. transfer the processing of personal data to a Sub-processor in a third country
  - c. have the personal data processed by the Data Processor in a third country
4. The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, is set out in Appendix C. 6.
5. The Terms may not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Terms cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

## **8. Assistance to the Data Controller**

1. Taking into account the nature of the processing, the Data Processor assists the Data Controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR.

This entails that the Data Processor should, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

- a. the right to be informed when collecting personal data from the Data Subject
- b. the right to be informed when personal data have not been obtained from the Data Subject
- c. the right of access by the Data Subject
- d. the right to rectification
- e. the right to erasure ('the right to be forgotten')
- f. the right to restriction of processing
- g. notification obligation regarding rectification or erasure of personal data or restriction of processing
- h. the right to data portability
- i. the right to object
- j. the right not to be subject to a decision based solely on automated processing, including

profiling

If the Data Processor receives requests directly from Data Subjects or Supervisory authorities regarding Personal Data processed on behalf of the Data Controller, the Data Processor shall: (i) direct such requests to the Data Controller without undue delay; (ii) not respond or act upon such requests without prior written approval from the Data Controller; and (iii) provide full cooperation as required under Art. 1 above.

2. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Term 6.4., the Data Processor should furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:
  - a. the Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
  - b. the Data Controller's obligation to without undue delay communicate the personal data breach to the Data Subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
  - c. the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
  - d. the Data Controller's obligation to consult the competent supervisory authority ('The Danish Data Protection Agency'), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.
3. The appropriate technical and organizational measures by which the Data Processor is required to assist the Data Controller as well as the scope and the extent of the assistance required is defined in Appendix C. This applies to the obligations foreseen under Term 9.1. and 9.2.

## 9. Notification of personal data breach

1. In case of a personal data breach, the Data Processor must, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.
2. The Data Processor's notification to the Data Controller should, if possible, take place within 48 hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR.
3. In accordance with Clause 9(2)(a), the Data Processor must assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) of the GDPR, must be stated in the Data Controller's notification to the competent supervisory authority:



- a. The nature of the personal data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;
  - b. the likely consequences of the personal data breach;
  - c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. All the elements to be provided by the Data Processor when assisting the Data Controller in the notification of a personal data breach to the competent supervisory authority is specified in Appendix D.

## **10. Erasure and return of data**

1. Upon termination of the personal data processing services, the Data Processor is under an obligation to either return or erase all the personal data to the Data Controller and delete existing copies unless Union or Member State law requires storage of the personal data including any hard-copy or electronic documents, as well as their copies on any medium or any derived materials containing such Personal Data, within thirty (30) business days after a request to return, delete or destroy the Personal Data for any reason, was submitted by the Data Controller;

## **11. Audit and inspection**

1. The Data Processor should make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Terms and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.
2. Procedures applicable to the Data Controller's audits, including inspections, of the Data Processor and Sub-processors are specified in Appendices C. 7. and C. 8.
3. The Data Processor is required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

## **12. Commencement and termination**

1. This DPA becomes effective on the date of both Parties' signature.
2. Both Parties are entitled to require the Terms renegotiated if changes to the law or inexpediency of the Terms should give rise to such renegotiation.
3. The Terms applies for the duration of the provision of personal data processing services. For the

duration of the provision of personal data processing services, the Terms cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 11.1. and Appendix C. 4., the Terms may be terminated by written notice by either Party.
5. Signature

On behalf of the **Data Controller**

Name  
Position  
Date  
Signature

On behalf of the **Data Processor**

Name  
Position  
Date  
Signature

### 13. Data Controller and Data Processor contacts/contact points

1. The Parties may contact each other using the following contacts/contact points:
2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name  
Position  
Telephone  
E-mail

Name:  
Position:  
Telephone:  
E-mail:

## Appendix A: Information about the processing

A1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

- a. To perform deliveries in accordance with the contractual obligations under the Master Agreement which in particular implies the Data Controllers' and its end users' allowance to use the Services owned and managed by the Data Processor;
- b. To offer support to the Data Controller and the end users of our Services
- c. To improve and develop the quality, functionality and user experience of our Services
- d. To detect, mitigate and prevent security threats and perform maintenance and debugging
- e. To prevent infringement and other abuse of our Services
- f. To process job applicants, follow-up communication and communication during processing of the job application
- g. To provide end users with service messages, updates and other relevant information relating to the use of or improved use of our Services

A2. The Data Processor's processing of personal data on behalf of the Data Controller should mainly pertain to (the nature of the processing):

The Data Processor makes the Services owned and managed by the Data Processor available to the Data Controller and thereby process personal data, primarily personal data of the 'end users' of the Services, as engaged by the Data Controller or other personal data as added by the Data Controller or its end user's, subject always to the limitation set out in A. 5.

A3. The processing includes the following types of personal data about Data Subjects:

A series of personal data is referred to as "Master Data" as the point of reference to end users' personal data at rest. The Master Data processed is agreed subject to information necessarily required to use the Data Processor's Services, which includes:

- Authentication i.e., end users' password
- Identification (such as names, company, technical pseudonym) to enable the identification of an end user interacting with the Services
- Contact information (such as email, phone number) to enable interaction with the Services
- Spoken language to localize the Services subject to the end users' choice

Other types of personal data processed by the Data Processor when the Services are being used:

- Behavior (product event logs, for example time of log in, time of file access) for the purpose to fulfil obligations of the Data Controller to log events
- Communication to allow messages to be sent through the Services owned and managed by the Data Processor
- Tracking IP-address identification is required in order to interact with the Services. IP-address, device ID and browser fingerprint are also used for debugging and may also be used as a technical measure to prevent fraud and malicious behavior (i.e., hacking). The IP-address is further used to approximate the geographical location of projects. Geolocation (GPS) is used to correlate the end users' current location with a position in a drawing or a map.

**A4. Processing includes the following categories of Data Subjects:**

- End users of the Services, including but not limited to employees and recruitment sourcing vendors and job applicants engaged by the Data Controller
- Individuals performing financial transactions with the Data Processor (i.e., purchasing the Services)

**A5. The processing of personal data should not include the processing of:**

- Special categories of Personal Data (Article 9 (1) of the GDPR)
- Personal Data relating to criminal convictions and offences (Article 10 of the GDPR)
- Personal Data regarding children (Article 12 (1) and Article 40 (2) (g) of the GDPR)
- Personal Data requiring special protection by the governing law

For the purpose of upholding the principles relating to processing of personal data in accordance with Article 5 (1) of the GDPR, the Data Processor severely encourages the Data Controller to instruct its end users to avoid or limit the inclusion of personal data when adding and uploading texts, images, documents, voice- and video memos to non-designated fields in the Service. Non-designated fields are fields without any explicit request to add, fill out or enter personal data, including without any limitation thereto, comment- and message fields or other “open” fields, where the aforementioned types of personal data can be added.

Where personal data is not limited to designated fields, the Data Processor will assist the Data Controller in moving, removing, or correcting the personal data towards a charge based on the available hourly consultancy rate of the Data Processor upon the time of request.

**A6. The Data Processor’s processing of personal data on behalf of the Data Controller may be performed when the Terms commence. Processing has the following duration:**

The processing of personal data is not time-limited and will be performed until the Master Agreement, or this DPA is terminated or cancelled by one of the Parties.

**A7. Access to personal data is provided to:**

- End users of the Data Controller as described under Appendix C, C.1.
- Relevant employees of the Data Processor who maintain compliance, development, sales, support, and marketing
- Contractors, consultants, and others who need access to the personal data in order to fulfill a contractual obligation of the Data Processor

**Appendix B Authorized Sub-processors****B1. The Data Processor’s use of Sub-processors**

The Data Controller agrees to give its general authorization for the Data Processor to engage Sub-processors to fulfill its contractual obligations towards the Data Controller under this DPA and the Master Agreement. Sub-processors may be used for the purpose of providing certain deliverables such as support and hosting services or other services subject to fulfilling the Data Processor’s contractual obligations. The current Sub-processors engaged by the Data Processor to carry out processing activities on behalf of the Data Processor are listed on the Data Processor’s website,

currently posted at: <https://www.squarecruit.com/intellectselect-privacy-policy/>

## B2. Prior notice for the authorization of Sub-processors

The Data Processor is obligated to inform the Data Controller before engaging a new Sub-processor to carry out processing activities on behalf the Data Processor. The Data Processor provides a registration mechanism on its website where the Data Controller can sign up to receive notices of changes and updates relating to the use of Sub-processors. All Sub-processor used by the Data Processor must comply with the relevant Terms put forward in this DPA.

## Appendix C Instruction pertaining to the use of personal data

### C1. The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller will be carried out by the Data Processor performing the following:

Ensuring required personal data of end users are available to other end users of the Services (through the user interfaces or application programming interfaces), for the purpose of enabling the end users to perform inspections, track document changes, log access, communicate and perform other tasks as provided by the Services on the data uploaded by the Data Controller (such as drawings, models etc.).

### C2. Security of processing

The level of security shall take into account:

- that the personal data does not involve special categories of personal data, personal data of minors or data requiring special protected by the governing law
- that the Master Data is the point of reference to end users agreed upon information
- that the Master Agreement may already describe that the Data Processor should establish a high level of data security

The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security appropriate to the risk.

The Data Processor should however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller (based on the risk assessment performed by the Data Controller:

- End user passwords are protected by using specialized hashing functions like Argon2, BCrypt or PBKDF2 to prevent Rainbow Table attacks
- Passwords in clear text must not be transferred over the internet
- Master Data should be separated from product data.
- The Data Processor must be able to restore personal data from a backup on daily basis
- Change of Master Data should be logged
- Employees with access to personal data must have signed a confidentiality agreement
- Access to Master Data is granted to employees in accordance with Appendix A
- Data transfer of personal data over the internet to the online services and products provided by the Data Processor should be performed securely (using HTTPS/TLS)

- The Data Processor must validate system integrity and security of updates to the services and products made available
- The Data Processor employ continuous self-evaluation to evaluate the organizational and technical measures used to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services

### C3. Storage period/erasure procedures

Upon termination of the Master Agreement the provision of personal data processing services ceases, unless stated and agreed otherwise in the Parties Master Agreement. The Data Processor should delete the personal data in accordance with the Master Agreement, or subject to any other written instruction submitted by the Data Controller.

### C4. Processing location

Processing of the personal data under this DPA cannot be performed at other locations than those described under Appendix B, B. 1, without the Data Controller's prior written authorization.

The Data Processor is entitled to outsource parts of its Services by employing or engaging Sub-processors to provide hosting, support, and other relevant services. The Data Processor aim to only appoint Sub-processors where processing of personal data is limited to the EEA. If not possible, the Data Processor rely on the following legal mechanisms when engaging any Sub-processor outside of the EEA, and when transferring personal data to such locations: *Countries deemed adequate by the European Commission, the European Commissions' Standard Contractual Clauses, approved binding corporate rules (BCR)* in accordance with Article 63 of the GDPR.

In addition, as regards to Sub-processors who provides hosting, the Data Processor should ensure that the hosting provider has an ISO 27001 revision statement or other equivalent standards that are substantial to ISO 27001 such as an ISAE 3402, or a type II revision statement on the basis of ISO 27001/2).

### C5. Instruction on the transfer of personal data to third countries

The Data Controller hereby instruct the Data Processor to make its Services available (e.g., mobile apps, web sites, application programmers' interfaces) to the Data Controller's end users, for the purpose of the ability to access, interact with, and transfer data from the Services. The instruction comprises that end users of the Data Controller should be entitled to access and transfer data to or when in a third country. The Data Processor will provide the data to the end user at the requested location and will restrict access only on the basis of authentication and authorization controlled from within the Services. Please note that geographical location is not available as an authorization measure.

Except as set forth in this section, the Data Processor will not transfer data to third countries.

### C6. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Controller or a representative of the Data Controller's should be entitled to, once a year, to perform inspection on the processing of personal data carried out by the Data Processor, including inspection on the Data Processor's physical facilities as well as systems used for and related to the processing to ascertain the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Terms.

The Data Controller's costs, if applicable, relating to physical inspection should be defrayed by the Data Controller. The Data Processor is, however, under an obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the inspection.

The Data Controller must notify the Data Processor prior to the performance of any inspection upon giving a 30 days' prior written notice.

#### **C7. Procedures for audits, including inspections, of the processing of personal data being performed by Sub-processors**

The Data Controller may – if required – elect to initiate and participate in a physical inspection at the Sub-processor's facilities. This may only apply if the Data Controller deems that the Data Processor's supervision of the Sub-processor has not provided the Data Controller with sufficient documentation to determine that the processing by the Sub-processor is being performed according to the Terms. The Data Processor's and the Sub-processor's costs related to physical supervision/inspection at the Sub-processor's facilities initiated by the Data Controller should be fully defrayed by the Data Controller.

#### **Appendix D Obligations of the Data Controller**

- D.1** The Data Controller is obliged to restrict and limit data input to the Services by instructing its end users to limit the adding of personal data to non-designated fields in the Services as specified in appendix A, A. 5.
- D.2** If the Data Controller engages a Sub-processor to use application programming interfaces (API) from the Data Processor's Services it is responsible to make sure and further require, that such Sub-processor, as a minimum, and subject always to a Sub-processor agreement, comply with the GDPR and the agreed Terms under this DPA, including all appendices thereto.

#### **Appendix E Limitation of liability**

- E.1** The Data Processor and the Data Controller is responsible for its own acts and omissions that may cause or result in a financial loss or fine as a consequence of its insufficient compliance with its obligations under this DPA and the GDPR. The Data Processor are not liable for any in-compliance or unlawful act by it if such act derives from instructions given by the Data Controller, or any act or omission of the Data Controller, provided that the Data Processor has fulfilled its obligations under Article 28 (3) of the GDPR.

The regulation of breach, responsibility, and limitation on liability in the Parties Master Agreement will apply to this DPA subsequently and as if this DPA was an integral part thereof. The Parties liability for all cumulated claims and damages that may arise under the duration of this DPA, is limited to the amount paid by the Data Controller over a three (3) month period to the Data Processor, based on the latest invoice issued to the Data Controller.