DALUX Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The company ordering products and/or services from data processor through entering into the Master Agreement as referred to in Appendix D

(the data controller)

and

The Dalux entity entering into the Master Agreement as referred to in Appendix D

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) , which are based on the Standard Contractual Clauses of the Danish Data Protection Agency, as approved by the European Data Protection Board, in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller. They are based on the Danish Data Protection Agency's Standard Contractual Clauses January 2020.

2. The Clauses have been designed to ensure the parties' 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 (General Data Protection Regulation).

3. In the context of the provision of the data processor's products and services and the data controller's use of the same, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. 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.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. 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.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall 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.

3. 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 the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

[1] References to ”Member States” made throughout the Clauses shall be understood as references to “EEA Member States”.

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 shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall 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. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall 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.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 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 shall implement appropriate technical and organisational 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. Pseudonymisation 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 organisational 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. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   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.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

   The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 60 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

3. 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 Clauses 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 organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

4. A copy of such a sub-processor agreement and subsequent amendments shall – 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 Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

5. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to 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.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations 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 organisations, 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 shall 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 from the data controller, the data processor therefore cannot within the framework of the Clauses:

    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 in 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, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational 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 shall, 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

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall 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, The Danish Data Protection Agency, 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 parties shall define in Appendix C the appropriate technical and organisational 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. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, 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 shall, 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 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall 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)GDPR, shall 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. The parties shall define in Appendix C 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.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to either delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses 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 shall be 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.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly

or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature of the Master Agreement referred to in Appendix D.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses 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 Clauses may be terminated by written notice by either party.

5. Signatures

   This data processing agreement is accepted by data controller when entering into the Master Agreement as referred to in Appendix D.

   Approved on behalf of the data processor by:

Name	Steffen Juhl Carlsen
Position	General Counsel
Date	15 May 2024

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the contacts/contact points stated below in 15.2.

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   Data controller
   The details of the data controller are specified in the Master Agreement as referred to in Appendix D.

   Data Processor
   Questions to the data processor regarding this data processing should be directed to the Dalux Privacy on the below details:

Telephone	+45 53 72 73 00

E-mail	privacy@dalux.com

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the processing of personal data is to deliver services and a system to support Building Information Modelling (BIM) for construction and facility management.

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 the data processor's Services
c) To improve and develop the quality, functionality, and user experience of the data processor's Services
d) To detect, mitigate and prevent security threats and perform maintenance and debugging
e) To prevent infringement and other abuse of the data processor's Services
f) To process orders, invoicing, payments, and other financial follow-ups
g) To provide end-users with service messages, updates, and other relevant information relating to the use of or improved use of the data processor's Services

A.2. The data processor's processing of personal data on behalf of the data controller shall 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 it's end user's, subject always to the limitation set out in A.3.

Access to personal data is provided to:

- End-users of the data controller as described under section A.4, e.g. user of the Services, a person using a graphical representation of the program (GUI) or a program using a programmatic representation (API). End-users are granted access by the data controller
- Relevant employees of the data processor who maintain compliance, development, sales and support
- Sub-processors, consultants, and others who need access to the personal data in order to fulfill a contractual obligation of the data processor.

A.3. 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 being processed and which is necessary to deliver the Services is the following::

- 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:
    - Behaviour (product event logs, for example, time of login, 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

- Financial transaction information processed when purchasing Services of the data processor. Some Services may also enable the data controller to manage their own financial transactions (i.e. invoices) which most likely will contain personal data of Data Subjects
- Tracking IP-address identification is required 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 behaviour (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 on a drawing or a map

The processing of personal data should not include:

- Special categories of Personal Data (Article 9 (1) of the GDPR)
- Personal Data relating to criminal convictions and offenses (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 the 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 all other fields where the adding of personal data is not specifically required to be added e.g. comment- and message fields, or other “open” fields, where 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 at the data processor’s currently applicable hourly rate for consultants at the time of the request.

A.4. Processing includes the following categories of data subjects:

- End-users of the Services, including but not limited to employees of the data controller and employees of any sub-contractors or third-party engaged by the data controller
- Individuals working on a construction or facility management site

A.5. The data processor’s processing of personal data on behalf of the data controller may be performed when the Clauses 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 data processing agreement is terminated or cancelled by one of the Parties.

Appendix B Authorised Sub-processors

B.1. Approved Sub-processors

The data controller consents to give its general authorization for the data processor to engage Sub-processors to fulfill contractual obligations towards the data controller under this data processing agreement and the Master Agreement.

Sub-processors may be used for the purpose of providing certain services such as support and hosting services or other services subject to fulfilling the data processor's contractual obligations.

The 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 at:

https://www.dalux.com/subprocessors/

As regards to Sub-processors who provide hosting services, the data processor ensures that the hosting Sub-processor holds an ISO 27001 revision statement or other equivalent standards, e.g. an ISAE 3402, or a type II revision statement on the basis of ISO 27001/2.

Data processor has entered into data processing agreements with its Sub-processors subject to the Sub-processors standard data processing terms which may not be based on these Clauses from the Danish Data Protection Agency.

B.2. Prior notice for the authorisation of Sub-processors

The data processor is obligated to inform the data controller before engaging a new Sub-processor in accordance with Clause 7.3. The data processor provides a registration mechanism on its website, via the link disclosed in B.1, where the data controller should sign up to receive the notices of changes and updates relating to the use of Sub-processors.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data controller gives the data processor the following instruction to process personal data:

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.).

C.2. 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 other personal data requiring special protection under the governing law
- that and the processing does not involve large amounts of personal data

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 upon) level of data security appropriate in relation to the risk.

The data processor should, however, in any event, and as a minimum, implement the following security measures agreed upon with the data controller (based on the risk assessment performed by the data controller):

The data processor has implemented policies, procedures, rules and controls covering the points described below regarding the security of processing. The data processor shall ensure that the points below are complied with in accordance with the Master Agreement including appendices, applicable laws, regulations and industry standards, including what is considered 'best practice' for the area/point in question.

1. Employees of the data processor who are engaged in the processing of personal data under the Clauses are subject to a duty of confidentiality. Only authorised personnel may have access to the personal data processed under the Clauses. If it follows from the Master Agreement that special security authorisations are required for staff engaged in the processing of the data controller's personal data, the data processor shall ensure that these authorisations are obtained.
2. The data processor has limited access rights to personal data. Access to personal data is limited to employees with a work-related need. Access is revoked when the user no longer fulfils the criteria for access. The data processor handles authorisation for the data processor's employees.
3. The data processor shall ensure that the data processor's employees receive relevant and sufficient training and instructions regarding security of processing.
4. The data processor uses appropriate logical authentication mechanisms, e.g. passwords, biometrics or similar. The authentication mechanisms used are based on best practice (e.g. requirements for the length and complexity of access codes and requirements for two-factor authentication).
    a. End-user passwords must be protected using specialised hashing functions such as Argon2, BCrypt or PBKDF2 to prevent Rainbow Table attacks.

   b. Plaintext passwords must not be transmitted over the Internet.

5. The data processor has appropriate technical and organisational measures to limit the risk of unauthorised access and/or installation of malicious code. Such measures may include firewalls, anti-virus software and malware protection. The data processor has formal procedures to ensure that security systems are kept up to date.
6. The data processor has formal change management procedures in place to ensure that any change is properly authorised, tested and approved prior to implementation. The procedure is supported by effective segregation of duties and/or management oversight to ensure that no single individual can control a change alone.
   a. The data processor shall validate the system integrity and security of the updates of the Services made available
7. The data processor shall use appropriate encryption technologies and other equivalent measures in accordance with applicable law, good data processing practice and industry standards for encryption of personal data.
   a. Personal data is encrypted during transport. The transfer of personal data over the internet to the data processor's Services must be secure (using HTTPS/TLS).
   b. To the extent agreed with the data controller, personal data is encrypted during storage.
   c. Decryption keys must not be stored together with the encrypted data.
8. The data processor shall ensure that systems and data are backed up and that backups are stored securely and in accordance with the Master Agreement. The same guidelines for backups apply as for all other processing of personal data under the Master Agreement and the Clauses.
   a. Database servers and web servers are separated, scaled and backed up separately. File data in the storage system is backed up immediately upon arrival. Backups are made at least daily. The data processor must be able to restore personal data from a daily backup.
   b. Limited access to backups is ensured.
   c. Backups are protected against deletion and manipulation.
   d. Backups must be stored physically separate from primary data
   e. The data processor shall not perform restores of personal data without prior authorisation from the data controller.
9. The data processor shall log all actions relating to personal data
   a. Logging is carried out at system and server/database level, respectively.
   b. Log data is stored for as long as it is relevant and then deleted. Log data is automatically deleted after 36 months.
   c. All actions regarding personal data such as login, search, view, creation, modification, export/extraction and deletion of data are logged.
   d. The logging of an action shall at least contain information about the time, user, action and indication of the data subject whose data it concerns or the search criterion used.
   e. Logging of rejected access attempts and blocking of further attempts shall be carried out after a specified number of consecutive rejected access attempts.
   f. Logging all actions related to the log, including changes to log setups and deactivation of logging.
   g. Logging of privileged/admin user actions.
   h. Ensure restricted access to the log.
   i. Log data is protected against deletion and manipulation.
10. Master Data must be separated from product data.

11. The data processor must ensure that development, production and testing take place in separate environments and that the data controller's personal data is not used for development and testing purposes.
12. The data processor shall have processes for handling data security breaches, cf. the provisions in 9.2.
13. The data processor has restrictions on physical access. Areas where personal data is processed - whether electronically or manually - are separated by access control mechanisms from areas to which there is general access.
14. The data processor shall ensure that data is erased before the data processor's equipment is handed over to a third party or otherwise disposed of.
15. The data processor shall ensure that the security of access to personal data is independent of whether work is carried out from the Data Processor's workplace or remote/home workplaces.
16. The data processor shall use ongoing self-assessment to evaluate the organisational and technical measures used to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

In addition, the data processor shall implement any measures that are separately agreed with the data controller.

C.3. Assistance to the data controller

The data processor shall insofar as it is possible and mutually agreed assist the data controller, subject to separate remuneration, in accordance with Clause 9.1. and 9.2. by implementing specific technical and organisational measures as requested by the data controller.

C.4. Storage period/erasure procedures

Unless other written instruction is given, the data processor continues to store the personal data upon termination of the Master Agreement, however reserves the right to delete the personal data three (3) months after termination of the Master Agreement.

C.5. Processing location

The processing of personal data by the data processor cannot be performed at other locations than at the data processor’s local offices within EEA, including in exceptional cases working from home, and those described under Appendix B, Clause B.1, without the Data Controller’s prior written approval.

C.6. Instruction on the transfer of personal data to third countries

The processing of personal data will include transfer of personal data to a third country outside of the EEA, as data processor’s Sub-processors, e.g. the support provider, operates and supports the platform from multiple locations. Such transfer is accepted by data controller, as data processor has documented an appropriately high level of security of data protection in accordance with Chapter V of the GDPR.

The transfer can only be made if the third country has been confirmed by the EU Commission to hold an adequate level of data protection, or the parties can ensure other appropriate safeguards pursuant to Article 46 of the GDPR (e.g. EU standard Contract Clauses (SCC), approved binding corporate rules, or any other current or future approved and valid legal mechanism, confirmed by the EU Commission). The legal basis for the transfer is described on data processor's website by following the link provided for in section B.1.

The data controller moreover instructs the data processor to make its Services available (e.g. mobile apps, websites, application programmers' interfaces) to the data controller's end-users, for 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 present 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.

C.7. 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 is entitled to once a year, to perform an inspection on the processing of personal data carried out by the data processor, including inspection of 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 inspection can also be conducted digitally by e.g. answering a questionnaire or similar provided by the data controller.

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.

C.8. 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 Clauses. The data processor's and the Sub-processor's costs related to a physical inspection at the Sub-processor's facilities initiated by the data controller should be fully defrayed by the data controller.

Appendix D The parties’ terms of agreement on other subjects

The Clauses in this data processing agreement 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’ latest executed Master Agreement.

In the event of data processor’s notification to the data controller of potentially unlawful instructions in accordance with section 4(2), the parties will in good faith negotiate to eliminate or mitigate the matter.

The data processor is not liable for any incompliance or unlawful act by it which may cause a breach of the GDPR or this data processing agreement if such acts derive from observations and instructions given by the data controller. The data processor can never be liable for the data controllers act and omissions, provided that the Data Processor has not violated its obligations under Article 28 (3) of the GDPR. In the event the data processor violates its obligations under this data processing agreement and such violation results in a liability for damages, the data processor’s total liability for all claims and damages will be limited to the amount paid by the data controller to the data processor over a three (3) month period, based on the latest invoice issued to the data controller.

The data processor and the data controller is responsible for its own actions and omissions that may cause or result in financial losses or administrate fines as a consequence of insufficient compliance with its obligations under this data processing agreement and the GDPR.