**DATA PROCESSING AGREEMENT**

("**Data Processing Agreement**")

This Data Processing Agreement is entered into by the the Customer and/or Value Chain Company (the "**Data Controller**") and Normative (the "**Data Processor"**) (each a "**Party**" and jointly the "**Parties**") in respect of Normative's Services and are incorporated into the Agreement between the Customer and/or Value Chain Company and Normative by reference in the General Terms and shall be construed in accordance with the General Terms available at www.normative.io/general-terms/ in the event that Normative is acting as a Processor to the Customer and/or Value Chain Company.

**Background:**

A. Normative and the Data Controller have entered into an agreement relating to Normative's provision of the Service via an Order Form or by accessing the Service and/or by reference on www.normative.io which incorporated the General Terms (the "**Main Agreement**").

B. When performing the contractual obligations in the Main Agreement, it is anticipated that Normative may Process Personal Data on behalf of the Data Controller. The Processing of such Personal Data by Normative is conducted on behalf of the Data Controller for which Normative is the Data Processor. This Data Processing Agreement regulates the terms and conditions for how Normative will Process Personal Data on behalf of the Data Controller as further detailed in **Appendix 1**.

C. If any provision of the Main Agreement conflicts with the terms of this Data Processing Agreement, the terms of this Data Processing Agreement shall take precedence to the extent its terms provide greater protection for Personal Data.

**1. Definitions**

1.1. In this Data Processing Agreement the following terms have the following meanings:

1.2. "**Agreement Date**" means the date that the Customer and/or Value Chain Company entered into an Order Form with Normative and/or accessed Normatie's website www.normative.io;

1.3. "**Processing**", "**Data Controller**", "**Personal Data**", "**Data Processor**", "**Personal Data Breach**", and "**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 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) (**"GDPR"**);

1.4. "**Data Processing Agreement**" means this Data Processing Agreement and all appendices attached hereto;

1.5. "**Applicable Laws**" means laws and regulations under EU law and relevant Member State laws that from time to time apply to the Data Processor and the Data Controller (including Applicable Data Protection Laws);

1.6. "**Applicable Data Protection Laws**" means from time to time applicable legislation and regulations, including regulations issued by relevant supervisory authorities, protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data that apply to Normative and the Data Controller, including data protection laws and regulations implementing the Data Protection Directive 95/46/EC and as of 25 May 2018 the GDPR;

1.7. "**Third Country**" means a country which is not a member of the European Union (EU) or the European Economic Area (EEA);

1.8. **"EU Processor-to-Processor Clauses**" means the standard contractual clauses between processors for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as at Schedule 1; and

1.9. "**EU Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as at Schedule 2.

1.10. When the context requires it, singular shall include plural, and vice versa, and the gender of each pronoun shall include all genes.

## 2. General Obligations for the Data Controller

2.1. The Data Controller shall in its role as the Data Controller ensure the compliance with the Applicable Data Protection Laws.

2.2. The Data Controller shall in accordance with Section 30 (1) in the GDPR provide the Data Processor records of processing activities that are required in order for the Data Processor to be able to comply with its obligation to maintain a record of processing activities in accordance with Section 30 (2) in the GDPR.

2.3. The Data Controller shall appoint a data protection officer and/or a representative if required by the Applicable Data Protection Laws and, where necessary, provide the Data Processor with the contact details to such person.

2.4. By entering into this Data Processing Agreement, the Data Controller confirms that the technical and organisational measures stated in **Appendix 2** are considered adequate and sufficient in order to protect the Personal Data covered by this Data Processing Agreement and that the Data Processor gives sufficient guarantees in accordance with Section 28 (1) in the GDPR.

## 3. Instructions

3.1. The Data Controller instructs the Data Processor to process Personal Data only on behalf of the Data Controller and in accordance with the instructions by the Data Controller, as set out in this Data Processing Agreement and the Main Agreement. The Data Controller ensures that the instructions comply with the Applicable Data Protections Laws.

3.2. If the Data Controller leaves instructions that go beyond what is stated in this Data Processing Agreement and the Main Agreement, the following shall apply. In the event the implementation of actions required by the instructions entail costs for the Data Processor, the Data Processor shall inform the Data Controller thereof and provide an explanation of why the actions entail costs. The Data Processor shall be required to implement the measures only on condition that the Data Controller confirms that the Data Processor shall bear the costs of the actions. The instructions must be submitted in writing, unless there are special reasons justifying that the instructions may be given orally, in which case the Data Processor shall document and confirm the instructions in writing without undue delay.

3.3. The Data Processor shall notify the Data Controller if the Data Processor considers that an instruction regarding the Processing of Personal Data given by the Data Controller would be in a breach of Applicable Laws (”**Challenged Instruction**”). The Data Processor will not in such a case be obliged to follow the Challenged Instruction unless the Data Controller maintains it and takes the responsibility for the Challenged Instruction. In such a case, the Data Processor shall take the measures required by the Data Controller provided that the measures do not concern: (i) implementation of technical and organisational measures; (ii) Data Subject’s rights; or (iii) appointing Sub-Processors. In case of disagreement, the Data Processor is entitled to seek guidance from the relevant supervisory authority. If such authority considers that the proposed measures are lawful, the Data Processor shall take them, in which case the Section 3.2 applies with regard to the costs for the measures. The Data Processor’s obligation to notify the Data Controller according to the first sentence in this Section shall not apply to the extent the Data Processor is prevented from doing so in accordance with Applicable Laws.

## 4. The General Obligations for the Data Processor

4.1. The Data Processor will Process Personal Data only in accordance with the written instructions issued by the Data Controller by this Data Processing Agreement and the Main Agreement.

4.2. Notwithstanding what is stated in Section 4.1 above, the Data Processor may Process the Personal Data to the extent it is necessary for the Data Processor in order to comply with legal requirements under Applicable Laws to which the Data Processor is subject. If so, the Data Processor shall inform the Data Controller of that legal requirement before the Processing, unless Applicable Laws prohibit the Data Processor from providing this information.

4.3. The Data Processor shall upon request by the Data Controller assist the Data Controller by providing with necessary information that the Data Processor has access to, in order for the Data Controller to be able to comply with its obligations to perform an impact assessment in accordance with Section 35 and consult the supervisory authority in accordance with Section 36 in the GDPR, regarding the Processing of Personal Data that is conducted in accordance with Data Processing Agreement. The Data Processor is entitled to compensation for the costs from the Data Controller for such measures. The Data Processor's obligation to assist the Data Controller is limited to such information that the Data Controller otherwise has no access to.

4.4. Normative will take reasonable steps to ensure the reliability of any persons authorised to process any Customer Data and shall ensure that all such persons have committed themselves to confidentiality.

## 5. Security measures

5.1. The obligation to implement technical and organisational measures to protect the Personal Data

5.1.1. The Data Processor shall implement appropriate technical and organisational measures in accordance with what is provided in **Appendix 2** to protect and safeguard Personal Data that is processed against Personal Data Breaches. The Data Processor shall have a right to change these measures under the condition that the changes do not result in worse protection of the Personal Data and at least reach the level of protection that follows from the Applicable Data Protection Laws. In case the Data Controller requests that the Data Processor shall take technical and organisational measures that are in addition to what is stated above in this Section 5.1.1, the Section 3.2 shall not be applied to the costs for such measures.

5.2. Access to Personal Data etc.

5.2.1. The Data Processor shall ensure that access to the Personal Data is limited to those employees of the Data Processor who need access to the Personal Data in order for the Data Processor to fulfil its obligations under this Data Processing Agreement and the Main Agreement as well as in order to perform their job duties.

5.2.2. The Data Processor shall ensure that all employees authorised to access and Process the Personal Data have committed themselves to confidentiality.

5.3. Personal Data Breach

5.3.1. In the event of a Personal Data Breach at the Data Processor, the Data Processor shall notify the Data Controller about the Personal Data Breach without undue delay after when the Data Processor became aware of such Personal Data Breach. Moreover, the Data Processor shall provide such information that follows from the information obligation in Section 33 (3) in the GDPR, that the Data Processor has access to and that the Data Controller cannot access by other means.

5.3.2. The notification to the Data Controller shall include the following information:

5.3.2.1. a description of the nature of the Personal Data Breach including the categories and number of Data Subjects concerned and the categories and number of Personal Data records concerned;

5.3.2.2. the likely consequences of the Personal Data Breach; and

5.3.2.3. a description of the measures taken or proposed to be taken by the Data Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.3.3. Where, and in so far as, it is not possible for the Data Processor to provide the above information in Section 5.3.2 above at the same time, the information may be provided in phases (without undue further delay).

## 6. Right to Audit and Inspection

6.1. Normative agrees to maintain its ISO 27001 certifications, when such certification is made available for the duration of Normative acting as a Data Processor to the Data Controller. Normative will use an external auditor to verify that its security measures meet ISO 27001 standards in accordance

with the ISO certification process. On Data Controller's written request, and subject to appropriate confidentiality obligations, Normative will make available to the Data Controller: (a) a copy of the current certificate in relation to ISO 27001 when made available to Normative; and (b) any information reasonably requested by the Data Controller concerning Normative's processing of Customer Data under the Main Agreement and this Data Processing Agreement.

6.2. Other than in the context of investigating a Personal Data Breach involving Customer Data, Data Controller agrees to exercise any right it may have to conduct an audit or inspection under Article 28(3)(h) (or the Standard Contractual Clauses, if applicable) by requesting the information outlined in paragraph 6.1.

## 7. Use of Sub-Processors

7.1. The Data Processor may engage outside sub-contractors, consultants or other third parties to Process Personal Data on behalf of the Data Controller ("**Sub-Processors**"). Moreover, the Data Controller may let the Data Processor enter into a data processing agreement on behalf of the Data Controller directly with Sub-Processors. Such data processing agreement with a Sub-Processor shall impose the Sub-Processor corresponding and not less restrictive obligations than what follows from this Data Processing Agreement.

7.2. The Data Processor shall, in the event the Data Processor engages a Sub-Processor without undue delay, provide the Data Controller with the information stated in **Appendix 1** in writing.

7.3. The Data Controller has a right to, by providing a cause within five (5) working days after the Data Processor has informed the Data Controller in writing about engaging a Sub-Processor, object to the Data Processor engaging the actual Sub-Processor. If the Data Controller has not objected within the stated time, the proposed Sub-Processor is deemed accepted. If the Data Controller objects to the Sub-Processor, the Data Processor has a right to choose one of the following alternatives: (a) refrain from engaging the Sub-Processor to process Personal Data covered by this Data Processing Agreement; (b) take measures that reasonably eliminate the reason for the Data Controller's objection; or (c) temporarily or permanently cease to provide the part of the service/services that entail Processing of Personal Data by the actual Sub-Processor. If none of these alternatives is feasible and the Data Controller maintains its objection after thirty (30) days has passed after the objection was made, each Party has a right to by giving a reasonable notice period terminate that part of the service/services that entails Processing of Personal Data by the actual Sub-Processor.

7.4. The Data Processor shall, in addition to the information stated in Section 7.2 above, upon the Data Controller's request provide information regarding the measures that have been taken to ensure that the Sub-Processor gives sufficient guarantees to implement technical and organisational measures in a way that complies with the requirements in Applicable Data Protection Laws.

7.5. The Data Processor is liable towards the Data Controller for the Processing of Personal Data by the Sub-Processors covered by this Data Processing Agreement in accordance with Applicable Data Protection Laws.

## 8. Liability

8.1. The terms and conditions regarding liability in the Main Agreement shall apply this Data Processing Agreement.

## 9. Data Subjects' Rights

9.1. The Data Controller shall be liable to assess if a request by a Data Subject to exercise its rights under Applicable Data Protection Laws is legitimate or not and provide the Data Processor with instructions regarding the scope of support that is stated below is required.

9.2. The Data Processor shall without undue delay inform the Data Controller about complaints and other notices from the Data Subjects exercising their rights. However, the Data Processor shall not, unless the Data Controller has given the Data Processor sufficient instructions thereof, communicate with the Data Subject.

9.3. The Data Controller is responsible for handling in connection with the Data Subject exercising its rights under Applicable Data Protection Legislation.

9.4. The Data Processor shall upon the request assist the Data Controller with following appropriate technical and organisational measures in connection with the Data Subject exercising its rights under Chapter III in the GDPR:

9.4.1. In connection with a request of *information* the Data Processor shall provide the Data Controller with such information that is covered by Sections 13 and 14 in the GDPR to the extent such information is available for the Data Processor and the Data Controller does not have access to such information.

9.4.2. In connection with a request of *right of access* the Data Processor shall provide the Data Controller with such information that is covered by Section 15 in the GDPR to the extent such information is available for the Data Processor and the Data Controller does not have access to such information.

9.4.3. In connection with a request of *rectification* (Section 16 in the GDPR), *erasure* (Section 17 in the GDPR), *restriction of processing* (Section 18 in the GDPR), and *data portability* (Section 20 in the GDPR), the Data Processor shall, to the extent the Data Controller cannot take the measures requested by the Data Subject(s), either by enabling the Data Controller to take such measures, or, if not possible, assisting the Data Controller to take such measures.

9.4.4. The Data Processor shall, on instructions for the Data Controller, notify the Sub-Processors that Process Personal Data covered by the request by the Data Subject to rectify, erase or restrict the processing (Section 19 in the GDPR) that such request has been made. The Data Controller undertakes to inform other recipients.

9.4.5. In relation to the Data Subject's right to object processing in Section 21-22 in the GDPR, the Data Controller shall assess whether the objection is legitimate and how it is to be handled. In the event the Data Controller wishes to be assisted by the Data Processor, the Data Controller shall issue further instructions, whereby the routines described in Section 3.2 shall apply to the Data Processor's right to compensation for costs.

9.5. In the event the Data Controller requests that the Data Processor shall take technical and organisational measures in addition to what is stated in Section 5.1.1 for the purpose of handling the Data Subject's rights under this Section 9, the Section 3.2 shall apply to the costs for such measures.

9.6. Notwithstanding what is stated above in Section 9.5, the Data Processor is entitled to compensation for reasonable expenses due to the Data Subject exercising its rights as set out above.

## 10. Return of Personal Data

10.1. Upon termination of the Main Agreement, the Data Processor shall return (and/or upon the Data Controller's written request in a secure and irreversible way delete or anonymise) all Personal Data which belongs to the Data Controller that the Data Processor and or any Sub-Processors have in its possession or control. This applies unless the Data Processor is required under Applicable Laws to continue to store the Personal Data.

## 11. Transfer to and Processing of Personal Data in a Third Country

11.1. The Data Processor may transfer Personal Data belonging to the Data Controller to a Third Country, provided that:

11.1.1. the Third Country provides an adequate level of protection for Personal Data in accordance with an adequacy decision issues by the EU Commission that covers the Processing of Personal Data;

11.1.2. the Data Processor ensures that there are appropriate safeguards in place in accordance with Applicable Data Protection Laws, e.g. standard data protection clauses adopted by the EU Commission under Applicable Data Protection Laws, covering the transfer and Processing of Personal Data; or

11.1.3. another exception exists under Applicable Data Processing Laws that covers the Processing of Personal Data.

11.2. For the avoidance of doubt, Personal Data may not be transferred to or Processed in Third Countries unless any of the conditions above in Sections 11.1 apply.

11.3. When a Customer and/or Value Chain Company is acting as a Controller and transfers Customer Data originating in the EEA, to a Processor located in a Third Country, the EU Controller-to-Processor Clauses will apply.

11.4. When Normative, its affiliates, or any other identified or unidentified third party is acting as a Processor and transfers Customer Data originating in the EEA to a Processor located in a Third Country, the EU Processor-to-Processor Clauses will apply.

## 12. Term and termination

12.1. This Data Processing Agreement will enter into force on the Agreement Date and is valid during the term of the Main Agreement or the longer period of time that the Data Processor or any Sub-Processor engaged by the Data Processor Processes Personal Data on behalf of the Data Controller.

## 13. Non-assignment

13.1. Neither the rights nor the obligations of either Party under this Data Processing Agreement may be assigned in whole or in part without the prior written consent of the other Party.

## 14. Amendments

14.1. Additions and amendments to this Data Processing Agreement shall be in writing and duly signed by both Parties to be valid. Each Party may request amendments to this Data Processing Agreement that are justified by changes in Applicable Data Protection Laws.

## 15. Applicable law

15.1. This Data Processing Agreement shall be governed by Swedish law, without the application of the choice of law rules, to the extent Applicable Data Protection Laws do not stipulate another law.

## 16. Disputes

16.1. Disputes arising out of this Data Processing Agreement shall be solved in Sweden to the extent Applicable Data Protection Laws do not stipulate another law.

* * * * * *

**Appendix 1**

**SCOPE, PROCESSING AND USE OF PERSONAL DATA COVERED BY THE DATA PROCESSING AGREEMENT**

This Appendix 1 shall be deemed to be an integral part of the Data Processing Agreement.

| ***Categories of Data Subjects*** | ***Categories of Personal Data*** | ***Processing Operations*** | ***Location, and, where applicable, safeguard for third country transfer*** | ***Retention of Personal Data*** |
|---|---|---|---|---|
| Customer Data which may include Customer's officers and Directors; Customer Employees, temporary workers, agents and volunteers, independent contractors engaged by the Customer; Customer's suppliers and vendors; advisors, consultants, and other professional experts engaged by the Customer and any other categories of Personal Data that may be contained in Customer Data. | Names, phone numbers, email addresses, address, and any other types of Personal Data that may be contained within the Customer Data | Normative will process Customer Data for the purpose of providing the Services to the Customer. | The Personal Data will be processed in Sweden. | Processor will retain the Personal Data according to instructions or for the longer time necessary in order for Processor to fulfil its obligations according to Applicable Laws.<br>We will retain the Personal Data for as long as there is a business relationship between the Parties and Normative requires the Personal Data in order to provide the Service. All Personal Data will be deleted upon termination of a business relationship in accordance with our data deletion policy of ninety (90) days. |

| | | | | |
|---|---|---|---|---|
| Customer Data which may include Value Chain Company's officers and Directors;  Value Chain Company Employees, temporary workers, agents and volunteers, independent contractors engaged by the Value Chain Company; Value Chain Company's suppliers and vendors; advisors, consultants, and other professional experts engaged by the Value Chain Company and any other categories of Personal Data that may be contained in Customer Data. | Names, phone numbers, email addresses, address, and any other types of Personal Data that may be contained within the Customer Data | Normative will process Customer Data for the purpose of providing access to the Service to the Value Chain Company. | The Personal Data will be processed in Sweden. | Processor will retain the Personal Data according to instructions or for the longer time necessary in order for Processor to fulfil its obligations according to Applicable Laws.<br>We will retain the Personal Data for as long as there is a business relationship between the Parties and Normative requires the Personal Data in order to provide the Service. All Personal Data will be deleted upon termination of a business relationship in accordance with our data deletion policy of ninety (90) days. |

Contact details of the contact person at the Data Processor: dpo@normative.io

## Appendix 2

## SUB-PROCESSORS

**Normative's sub-processors can be found at https://normative.io/sub-processors as updated from time to time.**

## Appendix 3

## TECHNICAL AND ORGANISATIONAL MEASURES

**Normative's Security Whitepaper acts as our technical and organisational measures which can be found at https://normative.io/security-whitepaper as updated from time to time.**

**Schedule 1**
**EU Processor-to-Processor Clauses**

This schedule is attached to and forms part of Normative's Data Processing Agreement with Customer and/or Value Chain Company governing the processing of Customer Data (the "**DPA**"). Unless otherwise defined in this schedule, capitalised terms used in this schedule shall have the meanings given to them in the DPA.

## SECTION 1

*Clause 1*
**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirement of Regulation (EU) 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 (**General Data Protection Regulation**)[1] for the transfer of personal data to a third country.

(a) The Parties:
  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter '**entity/ies**') transferring personal data, as listed in Annex I.A (hereinafter each '**data exporter**'), and
  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each '**data importer**')

have agreed to these standard contractual clauses (hereinafter: '**Clauses**").

(b) These Clauses will apply with respect to the transfer of personal data as specified in Annex I.B.

(c) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p.39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and processor pursuant to Article 29(3) of Regulation (EU) 2019/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

*Clause 2*
**Effect and invariably of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/697.

*Clause 3*
**Third-Party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8.1(a), (c), and (d) and Clause 8.9(a), (c), (d), (e), (f);
  (iii) Clause 9(a), (c), (d), and (e);
  (iv) Clause 12(a), (d), and (f);
  (v) Clause 13;
  (vi) Clause 15.1(c), (d), and (e);
  (vii) Clause 16(e);
  (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*
**Interpretation**

(a) Where these Clauses use terms that are defined in the Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with right and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*
**Hierarchy**

(a) In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*
**Description of the transfer(s)**

(a) The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7*
**Docking Clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and assigning Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II - OBLIGATIONS OF THE PARTIES**

*Clause 8*
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data

exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.[2]

**8.2 Purpose Limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

[2] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution of body, Article 29(4) of Regulation (EU) 2018/1725.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '**personal data breach**'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take

appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter '**sensitive data**'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter '**onward transfer**') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

1. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

transfer; (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

2. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

3. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*
**Use of sub-processors**

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the subprocessor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third party beneficiary rights for data subjects.[4] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a subprocessor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[4] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

*Clause 10*
**Data subject rights**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

*Clause 11*
**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*
**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*
**Supervision**

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Clause 14*
**Local laws and practices affecting compliance with the Clause**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred

personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[6];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

*Clause 16*
**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of

personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority and the controller of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where

(i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or

(ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*
**Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of The Kingdom of Sweden.

*Clause 18*
**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of The Kingdom of Sweden.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**
**ANNEX I**

**A. LIST OF PARTIES**
**Data exporter(s):**

**Name**: Normative AB "Normative" as identified in the Agreement.

**Address:** Åsögatan 108, 118 29 Stockholm, Sweden

**Contact person's name, position and contact details:** John Henry Mostyn, DPO, dpo@normative.io

**Activities relevant to the data transferred under these Clauses:** The activities specified in Appendix 1 of the DPA.

**Signature and date:** By transferring Customer Data to Third Countries on Customer's instructions, the data exporter will be deemed to have signed this Annex I.

**Role (controller/processor)**: Processor

**Data importer(s):**

**Name:**

**Address:**

**Contact person's name, position and contact details:**

**Activities relevant to the data transferred under these Clauses:** The activities specified in Appendix 1 of the DPA.

**Signature and date:** By receiving Customer Data on Customer's instructions, the data importer will be deemed to have signed this Annex I.

**Role (controller/processor):** Processor

**B. DESCRIPTION OF TRANSFER**

***Categories of data subjects whose personal data is transferred***
The Categories of data subjects are described in Appendix 1 of the DPA.

***Categories of personal data transferred***
The Categories of personal data are described in Appendix 1 of the DPA.

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***
The data exporter might include sensitive personal data in the personal data described in Appendix 1 of the DPA.

***The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).***
Personal data is transferred in accordance with Customer's instructions as described in paragraph 3 of the DPA.

***Nature of the processing***
The nature of the processing is described in Appendix 1 of the DPA.

***Purpose(s) of the data transfer and further processing***
To provide the Services.

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period***
The data exporter determines the duration of processing in accordance with the terms of the DPA.

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing***
The subject matter, nature and duration of the processing are described in paragraph 7 of the DPA.

## C. COMPETENT SUPERVISORY AUTHORITY

***Identify the competent supervisory authority/ies in accordance with Clause 13***
The Data Commissioner of the Kingdom of Sweden.

## ANNEX
## A. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

***Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.***
The technical and organisational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests are described in the DPA.

***For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.***
The technical and organisational measures that the data importer will impose on sub-processors are described in the DPA.

## ANNEX 15
## B. LIST OF SUB-PROCESSORS

***The controller has authorised the use of the following sub-processors:***
**Name:**

**Address:**

**Contact person's name, position and contact details:**

**Description of processing (including a clear delimitation of responsibilities in case several sub processes are authorised):** Sub-processors will process Customer Data to provide the Services in accordance with the details provided in paragraph 7 of the DPA.

**Schedule 2**
**EU Controller-to-Processor Clauses**

This schedule is attached to and forms part of Normative's Data Processing Addendum with Customer governing the processing of Customer Data (the "**DPA**"). Unless otherwise defined in this schedule, capitalised terms used in this schedule have the meanings given to them in the DPA.

## SECTION I

*Clause 1*
**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (**General Data Protection Regulation**)[7]for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter '**entity/ies**') transferring the personal data, as listed in Annex I.A (hereinafter each '**data exporter**'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each '**data importer**') have agreed to these standard contractual clauses (hereinafter: '**Clauses**').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

[7] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

*Clause 2*
**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*
**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13; (vi) Clause 15.1(c), (d) and (e);

(vi) Clause 16(e); (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*
**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*
**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*
**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*[Clause 7 – Optional]*
**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**8.1 Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '**personal data breach**'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU)

2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter '**sensitive data**'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter '**onward transfer**') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

1. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

3. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*
**Use of sub-processors**

(a) The data importer has the data exporter's general authorisation for the engagement of subprocessor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

[8] This requirement may be satisfied by the sub-processor accessing these Clauses under the appropriate Module, in accordance with Clause 7.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*
**Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*
**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[9] at no cost to the data subject. It shall inform the data subjects, in the

[9] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(e) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*
**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its subprocessor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor

acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

(a) Where the data exporter is established in an EU Member State: the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(c) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

*Clause 14*

**Local laws and practices affecting compliance with the Clause**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[10];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

---

[10] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data

exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

*Clause 16*
**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In

case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where
   (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or
   (ii) (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*
**Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Kingdom of Sweden.

*Clause 18*
**Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State. The Parties agree that those shall be the courts of the Kingdom of Sweden. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**
**ANNEX I**

**A. LIST OF PARTIES**
**Data exporter(s):**

**Name:** The entity identified as "Customer" in the Agreement.

**Address:** The address for Customer specified in the Agreement

**Contact person's name, position and contact details:** The contact details specified in the Agreement.

**Activities relevant to the data transferred under these Clauses:** The activities specified in Appendix 1 of the DPA.

**Signature and date:** By transferring Customer Data to a Third Country, the data exporter will be deemed to have signed this Annex I.

**Role (controller/processor):** Controller

**Data importer(s):**

**Name:** Normative AB "Normative" as identified in the Agreement.

**Address:** Åsögatan 108, 118 29 Stockholm, Sweden

**Contact person's name, position and contact details:** John Henry Mostyn, DPO, dpo@normative.io

**Activities relevant to the data transferred under these Clauses:** The activities specified in Appendix 1 of the DPA.

**Signature and date:** By receiving Customer Data on Customer's instructions, the data importer will be deemed to have signed this Annex I.

**Role (controller/processor):** Processor

**B. DESCRIPTION OF TRANSFER**
***Categories of data subjects whose personal data is transferred***
The Categories of data subjects are described in Appendix 1 of the DPA.

***Categories of personal data transferred***
The Categories of data subjects are described in Appendix 1 of the DPA.

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***
The data exporter might include sensitive personal data in the personal data described in Appendix 1 of the DPA.

***The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).***
Personal data is transferred in accordance with Customer's instructions as described in paragraph 3. of the DPA.

***Nature of the processing***
The nature of the processing is described in Appendix 1 of the DPA.

***Purpose(s) of the data transfer and further processing***
To provide the Services.

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period***
The data exporter determines the duration of processing in accordance with the terms of the DPA.

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing***
The subject matter, nature and duration of the processing are described in Appendix 1 of the DPA.

**C. COMPETENT SUPERVISORY AUTHORITY**
***Identify the competent supervisory authority/ies in accordance with Clause 13***
The Data Protection Commission of the Kingdom of Sweden

## ANNEX II
## A. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

***Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.***
The technical and organisational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests are described in the DPA.

***For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.***
The technical and organisational measures that the data importer will impose on sub-processors are described in the DPA.

## ANNEX III
## B. LIST OF SUB-PROCESSORS

**The controller has authorised the use of the following sub-processors:**

**Name:**

**Address**:

**Contact person's name, position and contact details:**

**Description of processing (including a clear delimitation of responsibilities in case several sub processes are authorised):** Sub-processors will process Customer Data to provide the Services in accordance with the details provided in paragraph 7 of the DPA.