DATA PROCESSING AGREEMENT

The following parties (collectively referred to as the "**Parties**" and individually "**Party**") have entered into the following data processing agreement (the "**DPA**") which consists of:

a) this master agreement;

b) Appendix 1: Supplementary information on the processing of the Controller's Data (as defined below); and

c) written amendments made in accordance with section 8 below.

PARTIES

1. _____
   _____
   _____
   (the "**Controller**"); and

2. DFRNT AB, company registration number 559395-0156, whose registered office is at Sankt Lars väg 41b, 22270 Lund, Sweden, with e-mail address info@dfrnt.com, a private limited liability company incorporated in Sweden (the "**Processor**").

The parties agree that this Data Processing Agreement ("DPA") sets forth their obligations with respect to the processing and security of Personal Data and, where explicitly stated in the DPA terms, customer data in connection with the online services provided by the Processor. The DPA (including its Appendix) is between the Processor and any customer receiving online services from the Processor based on the Terms and Conditions for DFRNT SaaS, and is incorporated by reference into the Terms and Conditions for DFRNT SaaS.

1. BACKGROUND, SCOPE AND TERMINOLOGY

1.1 The Parties have entered into one or more agreements that regulate the Processor's delivery and execution of one or more services for the benefit of the Controller (the "**Service Agreement**"). In connection with the performance of the Service Agreement, the Processor may process personal data for which the Controller is the data controller ("**Controller's Data**").

1.2 This DPA shall apply to all processing of the Controller's Data performed by the Processor on behalf of the Controller.

1.3 For the purposes of this DPA, "**Applicable Data Protection Law**" shall mean all EU legislation and other applicable national data protection laws and regulations applicable to the processing of the Controller's Data, including but not limited to the General Data Protection Regulation (EU 2016/679) ("**GDPR**") and the case law of the European Court of Justice in the application of the said legislation, as well binding instructions and decisions by competent supervisory authorities.

1.4 Terms used in GDPR such as the "data controller", "data processor", "personal data", "processing", "data subject", "binding cooperate rules", "personal data breach" and "supervisory authority" shall have the meaning as set out in GDPR.

1.5 If and to the extent the Processor is processing Personal Data on behalf and in accordance with the documented instructions of the Controller within the scope of the CCPA, the Processor makes the following additional commitments to the Controller. The processor will process the Personal Data on behalf of the Controller and will not

a. sell the Personal Data as the term "selling" is defined in the CCPA.

b. share, rent, release, disclose, disseminate, make available, transfer or otherwise communicate orally, in writing or by electronic or other means, the Personal Data to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions for cross-context behavioral advertising in which no money is exchanged.

c. retain, use or disclose the Personal Data for any purpose other than for the business purposes specified in the DPA Terms and the Terms and Conditions for DFRNT SaaS, including retaining, using or disclosing the Personal Data for a commercial purpose other than the business purposes specified in the DPA Terms or the Terms and Conditions for DFRNT SaaS, or as otherwise permitted by the CCPA.

d. retain, use or disclose the Personal Data outside of the direct business relationship with the Controller.

e. combine the Personal Data with personal information that it receives from or on behalf of a third party or collects from California residents, except that the Processor may combine Personal Data to perform any business purpose as permitted by the CCPA or any regulations adopted or issued under the CCPA.

2. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

2.1 The Controller (i) shall ensure that the Controller, when processing Controller's Data, complies with Applicable Data Protection Law; (ii) is at all times entitled to provide new or amended instructions regarding the processing of the Controller's Data, whereby the Processor shall be given reasonable time for implementation; (iii) shall without undue delay inform the Processor of any circumstances that may require modifications to the Processor's processing of the Controller's Data; (iv) is at all times entitled to, by written notification to the Processor, terminate the Processor's processing of the Controller's Data if the Controller has a reasonable grounds to believe that the Processor is unable, or has failed, to comply with the provisions of the DPA and/or Applicable Data Protection Law; and (v) provides a general authorisation to the Processor to engage Sub-Processors (as defined below), provided however that the Controller's authorisation is subject to such Sub-Processor's compliance with all the provisions set out in this DPA.

3. OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall process the Controller's Data only on behalf of the Controller and solely for the purposes specified by the Controller. In particular, the Processor shall:

a. Process the Controller's Data only in accordance with (i) this DPA; (ii) the instructions regarding processing of Controller's Data provided by the Controller; and (iii) Applicable Data Protection Law. If the Processor, in order to comply with Applicable Data Protection Law, is obliged to deviate from the provisions of this DPA and/or the Controller's instructions, the

Processor shall, without undue delay and before further processing of the Controller's Data, inform the Controller of such mandatory requirements, unless providing such information violates mandatory law.

b. Implement such technical, physical, administrative and organisational security measures as required by Article 32 GDPR and appropriate to the risk that the processing of the Controller's Data may impose on the rights and freedoms of data subjects. In assessing the appropriate security levels, and taking appropriate measures, the Processor shall ensure that account is taken in particular of the risks for accidental or unlawful destruction, loss or alteration and of the risks of unauthorised disclosure of, or unauthorised access to, the Controller's Data as well as of the risk of personal data breaches.

c. Ensure that individuals authorised to process Controller's Data have committed to confidentiality or are under an appropriate statutory confidentiality obligation.

d. Ensure that individuals processing Controller's Data has undergone relevant training in relation to the processing of the Controller's Data.

e. Assist the Controller by ensuring that the Controller's obligations under Applicable Data Protection Law and the DPA are complied with, for example, but not limited to regarding the performance of data protection impact assessments or audits performed by competent supervisory authorities.

f. Assist the Controller by implementing appropriate technical and organisational measures to comply with Controller's obligations in relation to data subjects' requests to exercise their rights under Articles 12-23 GDPR. The Processor shall without undue delay notify the Controller of such data subject requests. Unless explicitly stated in the Controller's instructions, provided for in mandatory law or a decision by a competent supervisory authority, the Processor may not respond to a data subject's request.

g. Without undue delay, provide the Controller with access to all information required to demonstrate that the Processor's obligations set out in this DPA and/or Applicable Data Protection Law have been fulfilled. The Processor shall also enable and contribute to the Controller's reviews of the Processor's processing of the Controller's Data, including audits of the Processor's premises, equipment and/or systems ("**Audits**"). The aforementioned shall also apply in relation to third parties authorised by the Controller to perform such reviews and audits on the Controller's behalf ("**Authorized Third Party**"), provided however that such Authorized Third Party (i) has executed a non-disclosure agreement appropriate for the purpose; and (ii) is not conducting operations that compete with the Processor's operations. The Controller is responsible for ensuring that reviews and Audits are carried out without unreasonable disruptions of the Processor's operations, including the activities performed by and for the benefit of the Processor's other customers and their reasonable need for protection of their operations. The Controller shall bear all Authorized Third Party costs as well as its own costs for reviews and Audits.

h. Keep a record in accordance with Applicable Data Protection Law on the processing of the Controller's Data under this DPA and allow the Controller access to such record at the Controller's request.

i. Ensure that the Controller provides written approval of transfer of Controller's Data to recipients outside the EU/EEA ("**Third Country**") before initiating such transfer. If the

Controller has submitted its written approval of transfer of Controller's Data to a Third Country, the Processor may perform such transfer only if the transfer is permitted according to Applicable Data Protection Law. The Processor shall, upon the Controller's request, provide the Controller with documentation and other information that may be required to demonstrate that the transfer is permitted according to Applicable Data Protection Law. If such transfer is possible only if the Controller enters into an agreement directly with a third party, the Controller commits to ensure that such agreement is executed.

j. Ensure that the Controller's Data is only transferred, disclosed, transmitted or otherwise made available by the Processor to other processors ("**Sub-Processors**") who, by agreement with the Processor, is bound by obligations that correspond to the Processor's obligations set out in this DPA. The Processor shall, at the Controller's request, provide to the Controller (i) a list of all Sub-Processors; and (ii) copies of agreements with the Sub-Processors. The Processor shall be liable for a Sub-Processor's processing of the Controller's Data and otherwise for the Sub-Processor's actions and omissions including, but not limited to, such liability as is regulated in clause 6 of this DPA, as if they were the Processor's own acts, omissions or defaults.

k. When replacing or hiring a new Sub-Processor, ensure that the Controller is given the opportunity to object to such change. If the Controller reasonably and fairly objects to the replacement or hiring of a Sub-Processor, the Processor shall ensure that the Sub-Processor's processing of Controller's Data is not initiated, or, where applicable, is terminated without unnecessary delay. The Controller acknowledges that an objection to a specific Sub-Processor may result in (i) limitations in the Processor's ability to comply with its obligations under the Service Agreement; and (ii) that the Processor may be entitled to compensation under clause 4.2.4.2d below.

l. Without undue delay inform the Controller if the Processor believes the Controller's instructions violate Applicable Data Protection Law or that Controller's Data is processed or may be processed in violation of Applicable Data Protection Law. The Processor is not entitled to stop the processing of the Controller's Data unless the Processor can reasonably demonstrate that continued processing would result in that the Processor would violate the DPA and/or Applicable Data Protection Law.

m. Without undue delay, inform the Controller of a competent supervisory authority's investigation or audit of the Controller's Data, unless providing such information violates mandatory law.

n. Without undue delay, notify the Controller of a suspected or confirmed personal data breach related to the processing of the Controller's Data. Such notice shall include information provided for in Article 33 (3) (a) (d) GDPR ("**Required Information**") and any other information that may be necessary for the Controller to be aware for the purpose of not jeopardising the rights and freedoms of data subjects, in their its right to protection of their personal data. If the Processor at the time of notification of a suspected or confirmed personal data breach cannot provide all the Required Information, the missing information shall be communicated to the Controller without delay and as soon as this information becomes available to the Processor. If it is likely that a suspected or confirmed personal data breach put data subjects' freedoms and rights at risk, the Processor shall, without undue delay, take appropriate measures to prevent and/or mitigate potentially adverse effects and consequences of

the breach.

o. In the event of termination of this DPA, depending on what the Controller requests, delete or return all the Controller's data, including copies thereof, provided however that the Processor is not prohibited by mandatory law to comply with the Controller's request.

3.2 If a review or an Audit of the Processor requested by the Controller according to clause 3.1.3.1g relates to something that is covered by an audit report made in accordance with SSAE 16/ISAE 3402 Type II, ISO, NIST or similar, the Controller shall the accept the results of that report instead of having the requested review or Audit being performed. The aforementioned shall apply only if (i) the audit report has been performed by an independent third party that can reasonably be assumed to possess relevant competencies; (ii) the Processor confirms that the reviewed functions, processes and measures have not changed after the completion of the audit report; (iii) the audit report has been completed no more than 12 months prior to the date on which the Controller has made his request for review or Audit; and (iv) both Parties consider that the procedure is consistent with Applicable Data Protection Law.

4. COMPENSATION

4.1 Unless otherwise agreed in writing between the Parties, the Processor shall not receive any compensation for the fulfilment of its obligations under this DPA, including compliance with the Controller's instructions regarding the processing of the Controller's Data, besides to the compensation received pursuant to the Service Agreement.

4.2 Notwithstanding clause 4.1 above, the Processor is entitled to compensation for actual and proven additional costs incurred by the Processor as a result of:

a. the Processor's assistance with data protection impact assessments pursuant to Article 35 GDPR initiated by the Controller;

b. the Processor's assistance on a review or an Audit of the Processor and/or its Sub-Processors initiated by the Controller, however no compensation will be paid for assistance on reviews or Audits that are performed in accordance with clause 3.2;

c. that the Controller, after the DPA has entered into force, notifies the Processor of new or changed instructions regarding the Processor's processing of the Controller's Data;

d. that the Sub-Processor's processing of the Controller's Data has been terminated at the Controller's request in accordance with clause 3.1.3.1k; and

e. that the extent of the Processor's assistance with regards to the Controller's compliance with Articles 12-23 GDPR substantially exceeds what the Processor could reasonably have foreseen at the time of the execution of the DPA.

5. CONFIDENTIALITY

5.1 The Parties hereby undertake, during the term of the DPA and for a period of 5 years thereafter, not to disclose to any third party information regarding the DPA, nor any other information which the Parties have learned as a result of the DPA, whether written or oral and irrespective of form ("**Confidential Information**"). The Parties agree and acknowledge that the Confidential Information may be used solely for the fulfilment of the obligations under the DPA and not for any other purpose. The receiving Party further agrees to use, and cause its directors, officers, employees, sub-contractors or other intermediaries

to use, the same degree of care (but not less than reasonable care) to avoid disclosure or use of Confidential Information as it uses with respect to its own confidential and/or proprietary information.

5.2 The provisions of clause 5.1 does not apply to information which

a. at the date of its disclosure is in the public domain or at any time thereafter comes into the public domain (other than by breach of this DPA); or

b. the receiving Party can evidence was in its possession or was independently developed at the time of disclosure and was not obtained, directly or indirectly, by or as a result of breach of a confidentiality obligation.

5.3 The confidentiality undertakings provided for in this section 5 apply to the extent that any Party is required to make a disclosure of information by law or pursuant to any order of court or other competent authority or tribunal or by any applicable stock exchange regulations or the regulations of any other recognised market place. In the event that any Party would be required to make any such disclosure, each Party undertakes to give the other Party immediate notice prior to any such disclosure, in order to make it possible for the other Party to seek an appropriate protective order or other remedy. The Parties also agree and undertake to use their best efforts to ensure that any information disclosed under this section, to the extent possible, shall be treated confidentially by anyone receiving such information.

6. LIABILITY

6.1 Subject to clause 6.2 below, each Party is liable for administrative fines pursuant to Article 83 GDPR ("**Administrative Fines**") that are imposed on the Party in question ("**Fined Party**").

6.2 To the extent that the Fined Party, for example, but not limited to, by virtue of a legally enforceable Administrative Fine, can reasonably demonstrate that the Administrative Fine, in whole or in part, has been imposed on the Fined Party due to deficiencies of the other Party, the other Party shall compensate the Fined Party with an amount corresponding to the portion of the Administrative Fine that can reasonably be attributed to said deficiencies.

6.3 A Party ("**Defaulting Party**") shall indemnify the other Party in relation damages imposed on the other Party due to Data Subject Claims that stems from a court decision, arbitration or settlement, as well as the other Party's costs associated with such Data Subject Claims. For the purposes of this DPA, "**Data Subject Claims**" shall mean claims according to Article 82.1 GDPR, where the claims are resulting from the Defaulting Party's failure to fulfil its obligations under this DPA and/or applicable Data Protection Law.

6.4 The Defaulting Party's liability pursuant to clause 6.3 is subject to (i) that the Defaulting Party, without undue delay, has been informed by the other Party of the Data Subject Claims; and (ii) that the Defaulting Party - after due consultation with the other Party – is granted exclusive rights to handle all aspects of the claim in court proceedings and/or negotiate a settlement ("**Process Control**"). If the other Party can reasonably demonstrate that its intellectual properties, brand reputation or similar can be compromised by transferring the Process Control to the Defaulting Party, the other Party has the right to refrain from such a transfer, whereby the Defaulting Party's liability shall be limited to the lower amount of (i) what may reasonably be assumed to have been the outcome if the transfer of Process Control had been completed; and (ii) the compensation paid by the other Party to data subjects as a result of the Data Subject Claims.

6.5 The Parties' liabilities set out in clauses 6.3 and 6.4 shall in any event be limited to an amount corresponding to 100 % of the fees received by the Processor for services rendered under the Service Agreement for the last 12 months prior to the incident that caused the claim.

6.6 The limitations of liability set out in this section 6 shall not apply to claims under Article 82.5 GDPR.

6.7 Neither Party is liable for indirect damage or consequential loss such as, for example, but not limited to, lost revenue, loss of profit or goodwill unless the damage resulted from to a Party's gross negligence or intent.

6.8 In the event of any discrepancies between the liability provisions of this DPA and the provisions of the Service Agreement, the provisions of this DPA shall prevail.

7. TERM AND TERMINATION

7.1 This DPA shall enter into force upon signature by both Parties and shall remain in force until terminated in accordance with the provisions of this section 7.

7.2 This DPA will terminate at the later date of (i) the date of termination of the Service Agreement; and (ii) the date on which the Processor ceases to process the Controller's Data.

7.3 Notwithstanding clause 7.2, each Party is entitled to terminate the DPA with immediate effect if the other Party commits a material breach of contract and does not rectify it within 30 days after written request thereof.

8. CHANGES AND AMENDMENTS

8.1 Any changes to and/or amendments to this DPA shall be in writing and signed by both Parties in order to be valid.

9. GOVERNING LAW

9.1 This DPA shall be governed by and interpreted in accordance with Swedish law.

*****

This DPA is referenced by Terms and Conditions for DFRNT SaaS.

APPENDIX - SUPPLEMENTARY INFORMATION

Supplementary information concerning the processing of Controller's Data

1. CONTENT AND SCOPE

This Appendix 1 contains:

a. the scope and purpose of the processing of Controller's Data;

b. categories of data subjects;

c. categories of personal data;

d. whether Third Country transfer has been approved by the Controller;

e. contact details of the Parties; and

f. additional instructions.

2. SCOPE AND PURPOSES, CATEGORIES OF DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA

2.1 Nature and purpose

Nature of the processing
Administrative processing of personal data to uphold the services provided by the Processor in connection with agreements between the Processor and Controller..

Purpose of the processing
Enable processing of personal data related to website visits, user registration, use of digital products, licensing of digital products or in making a purchase through websites operated by the Processor..

2.2 Categories of data subjects

The following categories of data subjects' personal data may be processed:

- Employees
- Visitors
- Customers
- Suppliers
- Job applicants

2.3 Categories of personal data

General

The following categories of personal data may be processed:

- Identity data (e.g. first and last name)
- Contact details (e.g. address, phone number, e-mail)

- Customer relation management data (orders, invoices, purchase history etc.)

Special categories of personal data and other sensitive data

The following special categories of personal data may be processed:

- None

3. CONTROLLER'S APPROVAL OF THIRD COUNTRY TRANSFER OF CONTROLLER'S DATA

By signing the DPA, the Controller is providing its written approval to transfers of Controller's Data to Third Countries. The Processor acknowledges that the Controller's approval is conditional upon the Processor's compliance with the provisions of the DPA.

4. CONTACT DETAILS

The following contact information should be used for messages and other notifications required for the compliance with the DPA.

Notices to the Controller:

Postal address: Same as on service agreement

Email address: Same as for the individual user account created in service agreement

Contact person (if any): Same as for the individual user account created in service agreement

Notices to the Processor:

Postal address: DFRNT AB, Sankt Lars väg 41b, 22270 Lund, Sweden

Email address: privacy@dfrnt.com

Contact person (if any): Data Protection Officer

5. ADDITIONAL INSTRUCTIONS

For the avoidance of doubt, it is noted (i) that the Controller, after the DPA has entered into force, is entitled to issue amended instructions or add new instructions for the processing of the Controller's Data; and (ii) that such instructions shall be binding upon the Processor, provided however that the instructions have (a) been submitted in writing; (b) on another permanent medium; or (c) otherwise have been perceived and confirmed by the Processor.

When this DPA enters into force, no additional instructions are provided through this DPA.