Data Processing Agreement

1. Background

The Supplier and the Customer have entered into an agreement that includes the service(s) listed in the main agreement (the "**Agreement**") purchased by the Customer (the "**Services**"). Under the Agreement and in accordance with this DPA (as defined below), Supplier will from time to time and on behalf of the Customer process personal data for which the Customer is the controller.

2. Definitions

"**Applicable Data Protection Legislation**" means, unless otherwise agreed in writing between the Parties; (i) the General Data Protection Regulation, (ii) the national data protection legislation in Sweden; Denmark, Norway and/or Finland, as applicable for the Services; and (iii) the Data Protection Authority regulations and decisions applicable to the processing of personal data under this DPA in Sweden, Denmark, Norway and/or Finland, as applicable.

"**Customer Equipment**" means computers and other equipment owned, rented or leased by the Customer or the Customer's operations provider.

"**Supplier**" means the relevant Dustin company within the Dustin group, as listed in Appendix A, and where relevant each person/entity authorized to perform work on behalf of a company listed in Appendix A.

"**Supplier Equipment**" means computers and other equipment owned, rented or leased by the Supplier or the Supplier's operations provider.

"**DPA**" means this data processing agreement and attached appendices, as well as all changes thereto resulting from provisions of the Agreement.

"**Security Measures**" means the appropriate technical and organizational measures necessary to comply with Applicable Data Protection Legislation, listed in Appendix A or otherwise necessary to protect the personal data being processed from data breaches.

"**Standard Contractual Clauses**" means (i) the EU standard contractual clauses as adopted by the European Commission decision 2021/914 of 4 June 2021; (ii) to the extent applicable, any future European Commission decision amending or replacing this decision; or (iii) during any grace period granted under such applicable decision, the previous version thereof.

"**Third Country**" means a country outside EU/EEA.

3. Processing of personal data

3.1 *Instructions*

The Customer is responsible for the processing of personal data being carried out in compliance with the Applicable Data Protection Legislation in its capacity as controller. The Customer must ensure that the Supplier does not process other categories of personal data on behalf of the Customer than the categories of personal data listed in Appendix A for the relevant Services and within the scope stated therein. Unless otherwise specifically stated in Appendix A, the Supplier shall when providing IT consultancy services:

(a) only process personal data with regard to the categories of data subjects within the scope of the Services by nature considered as harmless, such as contact information for customers and employees; and
(b) not process personal data constituting special categories of personal data, such as health data or other sensitive data.

The Supplier only process personal data in accordance with documented instructions of the Customer, unless the Supplier is otherwise obligated to process personal data under Swedish, Danish, Norwegian, Finnish and/or EU law, as applicable. In such cases, the Supplier will, to the extent allowed under applicable law, inform the Customer of such legal obligations before the processing is commenced.

Either Party must ensure that the other Party has the right to process contact information and other types of personal data of the other Party's employees if and to the extent such processing is necessary to provide the Services.

The Supplier may not process personal data for its own purposes or other purposes except as set out in the DPA and the Agreement. The Supplier is entitled to process personal data for the purposes of providing, maintaining and providing support for the Services.

This DPA and the Customer's use of the Services are the Customer's complete and final instructions to the Supplier with regard to processing of personal data, with the exception of any written instructions the Customer is obliged to provide Supplier in order to comply with Applicable Data Protection Legislation. Any other changes must be agreed separately in writing between the Parties, including but not limited to changes relating to Appendix A. If the Supplier accepts the adjusted instructions, the Supplier is entitled to reasonable compensation for adapting to such instructions. If the Supplier informs the Customer within reasonable time that it cannot comply with the Customer's adjusted instructions made in order to comply with Applicable Data Protection Legislation, the Supplier is not bound by the proposed instructions and the Customer is entitled to terminate the Agreement in accordance with section 11.2.

3.2 *Security Measures*

3.2.1 *General*

The Supplier has implemented and follows the Security Measures listed in Appendix A or stated in the Agreement when providing the Services. The Supplier's at all times applicable in-house IT safety regulation applies to the delivery of the Services, and the Supplier may adjust such regulations during the term of the Agreement.

The Customer is responsible for ensuring that the Security Measures fulfils the Customer's obligations related to adequate safety for the personal data being processed under Applicable Data Protection Legislation. If the

Customer requests a change of the Security Measures, the same provisions apply as for changed instructions requested by the Customer under the last paragraph of section 3.1. If the Supplier request changes to the agreed Security Measures, the paragraph below applies.

If the Supplier becomes aware that the Security Measures completely or partially are in breach of Applicable Data Protection Legislation, the Supplier will within reasonable time inform the Customer and provide adjusted written instructions on adequate Security Measures in accordance with the above for the Customer's approval. Should the Customer not approve the adjusted instructions within reasonable time after the Supplier has informed the Customer of the need of adjusted instructions, the Supplier is entitled to, at the expense of the Customer, take reasonable and necessary Security Measures to comply with Applicable Data Protection Legislation.

3.2.2 *Specific terms relating to IT consultancy services*

If and to the extent the Supplier provides IT consultancy services on Supplier Equipment or the Customer Equipment, the above under heading "General" applies also for such processing activities. However, as regards processing performed on Customer Equipment, the Customer is responsible for implementing necessary Security Measures.

4. Reporting of data breaches

If the Supplier becomes aware of a data breach, the Supplier must inform the Customer without undue delay and in accordance with Applicable Data Protection Legislation.

5. Sub-processors and transfers to third countries

The Supplier may engage another processor ("sub-processor") to process the personal data pursuant to this DPA, both within and outside the EU/EEA, provided that (i) such engagement will be under a written contract, and (ii) such subcontract will require the sub-processor to comply with essentially the same obligations as applicable to the Supplier under this DPA. Current list of sub-processors and countries where personal data can be processed can be found in Appendix A. The Supplier shall remain fully liable to the controller for the performance of that sub-processor's obligations. However, in respect of [Microsoft, LogMeIn, SkyKick and AppDirect, as applicable], Customer acknowledges and agree that the Supplier is not responsible for, nor obligated to force these service providers to comply with, other obligations regarding processing of personal data than as set out in the respective service provider's own terms and conditions as offered when using their services. Upon request, and to the extent possible under confidentiality obligations, the Supplier shall keep the Customer informed about the content of such agreements.

The Supplier will inform the Customer of any intended changes of any sub-processor by giving the Customer prior written notice thereof. The notice will include (i) the name of the sub-processor, (ii) the purpose for which it will be engaged, (iii) the location of the sub-processor and where the personal data may be processed and, where relevant (iv) transfer mechanism relevant for the Third Country transfer. The Customer has the right to submit a written objection to the change within fourteen days from receipt of notice. Should the Supplier despite the Customer's objection still wish to make the change, the Customer is entitled to terminate the Agreement in accordance with section 11.2.

The Supplier must ensure that there is a valid transfer mechanism in place for a transfer of personal data to a Third Country. Such transfer mechanism may be Standard Contractual Clauses or other equivalent provisions under Chapter V of the GDPR, as applicable from time to time.

In case of transfers of personal data to a Third Country and to the extent the Standard Contractual Clauses are applied as a legal basis for transfer of personal data to a Third Country, the Supplier or the sub-processor as applicable, may at its sole discretion determine which version and which modules of the Standard Contractual Clauses that are relevant and are to be used in each case, typically the modules for processor-to-processor transfers.

To the extent legally required, the Supplier will perform a risk assessment in relation to a transfer of data to a Third Country. Should the requirement to perform such assessment instead lay with a sub-processor appointed by the Supplier, the Supplier will request that the sub-processor performs such assessment. Some sub-processors may publish information in this regard, such as risk assessments, on their respective websites which lays beyond the Supplier's control. The Customer hereby acknowledges that such information, including any assessments made, lays beyond the Supplier's control and, for use of the Services, it is accepted.

The Customer is responsible for ensuring that the risk assessment performed, and any potential supplementary measures in place, fulfil the Customer's requirements related to adequate safety for the personal data being processed under Applicable Data Protection Legislation. Upon the Customer's reasonable request, the Supplier undertakes to provide sufficient information to the Customer for evaluating any risk assessment performed. In case the Supplier makes any changes to assessments made after entering into the Agreement, or engages a new sub-processor, and the Customer finds that the updated or new assessment does not fulfil its obligations under Applicable Data Protection Legislation, the Customer may submit a written objection to the use of the relevant sub-processor. Such objection should include information on the reasons as to why and how the assessment does not fulfil the Customer's obligations. The Supplier will then take such objection into consideration and, to the extent the Supplier deems it possible and necessary, update the assessment and potential measures taken based on the assessment. However, should the Supplier in its sole discretion determine that it is not possible or not reasonably necessary to make such changes, and the objections presented by the Customer include valid reasons (as defined under section 11.2), the Customer is

entitled to terminate the Agreement in accordance with section 11.2.

6. Assistance with requests from data subjects

In addition to what follows from section 3.2, the Supplier must implement adequate technical and organizational measures in order to, at the written request of the Customer, be able to assist the Customer in fulfilling the rights of the data subjects as set out in the General Data Protection Regulation. The Supplier's obligation under this provision only applies to the extent such assistance is reasonably possible and to the extent the processing of personal data requires such obligation. As regards IT consultancy services, the Customer shall at the latest upon signing the Agreement inform the Supplier in writing if and to what extend the Customer finds such measures necessary for the processing of personal data which the Supplier will carry out on behalf of the Customer when performing the IT consultancy services covered by the Agreement.

In addition to the above and taking into consideration the nature of the processing and the information available to the Supplier, the Supplier must at the written request of the Customer assist so that the Customer can fulfil the obligations imposed on it related to safety for personal data, data breaches, data protection impact assessment and prior consultation in accordance with Applicable Data Protection Legislation.

The Supplier is entitled to reasonable compensation for the assistance provided under this section 6.

7. Confidentiality and disclosure of personal data

Personal data, for which the Customer is controller and which the Supplier is processing in accordance with this DPA, is subject to the terms of confidentiality in the Agreement.

The Supplier must not disclose the Customer's personal data under this DPA to a data subject or a third party, unless otherwise stated in the Agreement or provided by law, a judicial decision or an official decision. If the Supplier discloses such information due to legal requirements, a judicial decision or an official decision, the Supplier will inform the Customer of the disclosure unless prohibited by the law, judicial decision or official decision in question.

The Supplier must without undue delay inform the Customer if the data subject requests information related to the processing of personal data under this DPA and refer the data subject to the Customer. The Supplier will assist the Customer in responding to such requests in accordance with section 6 above.

The Supplier and its representatives are obligated under Applicable Data Protection Legislation to co-operate with competent supervisory authorities. The Supplier will inform the Customer of such request without unreasonable delay if the request specifically concerns the processing of personal data under this DPA. The Supplier will not represent the Customer or act on behalf of the Customer in such requests from a supervisory authority. The Supplier is entitled to reasonable compensation for its work with inquiries related to the Customer subject to the inquiry not resulting from Supplier's breach of its obligations under this DPA.

8. Compensation

In addition to what is stated in this DPA, the Supplier is entitled to reasonable compensation for complying with the Customer's written instructions, unless the requested action is specifically stated in the Agreement. If the Supplier is entitled to compensation for work performed, Supplier's current price list will apply unless otherwise stated in the Agreement.

9. Liability

9.1 *General*

If the Supplier is liable to pay damages to data subjects in accordance with Applicable Data Protection Legislation, and the Customer has participated in the processing of personal data that forms the basis of the data subjects' claims, the Customer must reimburse the Supplier for the part of the damages that the Supplier is obligated to pay to data subjects that is attributable to the Customer's non-performance of its obligations or the Customer's instructions to the Supplier. In addition, the Customer must reimburse Supplier for its reasonable costs relating to the Supplier's defense against claims from data subjects (including what Supplier has been ordered to pay to data subjects).

If the Customer is liable to pay damages to data subjects in accordance with Applicable Data Protection Legislation, and the Supplier has participated in the processing of personal data that forms the basis of the data subjects' claims, the Supplier must reimburse the Customer for the part of the damages that the Customer is obligated to pay, and which is attributable to the Supplier's non-performance of its obligations under Applicable Data Protection Legislation or this DPA. In addition, the Supplier must reimburse the Customer for its reasonable costs relating to the Customer's defense against claims from data subjects (including what the Customer has been ordered to pay to data subjects). The Supplier's total liability under this DPA is limited to 150 percent of the service fee for the first twelve months of the Services, unless the Supplier has caused the damage by intent or gross negligence.

A Party's liability for damages not expressly stated herein is governed by the Agreement.

9.2 *Notification, right of information etc.*

A Party that is subject to claims from data subjects must within reasonable time (i) inform the other Party in writing of any claims made that may result in claims against the other Party pursuant to this section 9; and (ii) allow the other Party insight to the documents in such proceedings, both from the Party and from the data subjects, and allow the other Party to submit comments to such documents.

Claims for reimbursement under this section 9 are subject to compliance with the provisions above and may be raised no later than six months after a Party has been obliged to pay damages to data subjects.

10. Audits

The Supplier will provide the Customer access to any information which may reasonably be needed to prove that the obligations imposed upon processors under Applicable Data Protection Legislation have been fulfilled. This includes providing reasonable assistance in audits and inspections carried out by the Customer or an auditor appointed by the Customer. Inspections may only be done if an audit cannot be completed by the Supplier's disclosure of information. Supplier must be informed about an inspection in good time prior to the intended date of inspection with specification of the scope and purpose of the inspection. The Supplier is entitled to reasonable compensation for the costs associated with the implementation of such audit or inspection.

Prior to an audit or inspection, the Customer or the auditor appointed by the Customer must meet the necessary confidentiality obligations and comply with the Supplier's security regulations at the place of inspection. The inspection must not hinder the Supplier's business or risk the protection of other customers' information. Information gathered as part of the audit must be deleted after completed audit or when it is no longer necessary for the purpose of the audit.

11. Term and termination

11.1 *General*

This DPA is valid as long as the Supplier processes personal data on behalf of the Customer and terminates automatically in connection with the Agreement when the Supplier no longer provides any Services to the Customer. However, a Party's liability under this DPA applies also after the termination of this Agreement.

Upon termination of this DPA, the Supplier must delete or return the Customer's personal data to the Customer or to a third party at the instruction of the Customer, including data being processed on Supplier Equipment but excluding data being processed on Customer Equipment. The personal data stored electronically may be provided electronically according to the Customer's instructions, if reasonable. The Customer's request of deletion or return must be submitted within sixty days of the termination of this DPA. After expiration of the period above, and unless otherwise required under Swedish, Danish, Norwegian, Finnish and/or EU law, as applicable, the Supplier may delete existing copies of the personal data. After the return of the personal data, or if the return of personal data has not been requested by the Customer after the expiration of the above period, the Supplier will delete the Customer's personal data within reasonable time, but no later than six months after the termination of this DPA.

After the termination of this DPA, the Supplier may not process personal data for any other purpose than to delete the personal data or to protect the personal data from data breaches, unless otherwise required under Swedish, Danish, Norwegian, Finnish and/or EU law, as applicable. The Supplier has the right to reasonable compensation for the work performed under this section 11.1.

11.2 *Consequences of early termination*

The Customer is entitled to terminate the Agreement in accordance with section 3.1 and 5 relating to the Services affected, with a 90 days' notice period. If partial termination is not possible for technical reasons, then termination of any Service may apply to the entire Agreement and/or all Services affected. If the Agreement is terminated in accordance with above, the Supplier will refund any fees already paid for Services that will not be used after the termination of the Agreement. If the Customer has valid reasons for objecting, the Supplier may not hire the new sub-processor in question for the termination period. If the Customer cannot show that it has valid reasons for objecting, the termination is considered as an early termination without valid reason, in which case the Supplier is entitled to compensation corresponding to twenty-five percent of the remaining contract value. In addition, if the Services include products necessary for the delivery of the Services which have been purchased by the Supplier specifically for the Customer, the Customer undertakes to purchase such products from the Supplier, if Customer requests early termination in accordance with this section. As an example, such products may include network products owned or leased by the Supplier and installed at Customer sites, but do not include products related to private or public cloud services which are installed at the Supplier's or its partners premises.

"Valid reason" for the purpose of this section means circumstances on the part of the sub-processor that significantly affects, or is likely to affect, the protection of data subjects' personal data, such as a new sub-processor failing to comply with obligations imposed on processors under Applicable Data Protection Legislation.