SkyKick Data Processing Addendum

Last updated: January 17, 2023

This Data Processing Addendum (the "**DPA**") is entered into between the customer ("**Customer**") and SkyKick LLC, if Customer is based in the United States of America or SkyKick B.V. if the Customer is located outside the United States of America (each "**SkyKick**"). This DPA amends and forms a material part of the Agreement, pursuant to which Customer has obtained the right to use one or more Services.

1. DEFINITIONS AND BACKGROUND

1.1. **Definitions.** Capitalized terms used but not defined herein or in **Attachment 1** to this DPA will have the meanings set forth in the Terms and Conditions.

1.2. **Background**. Customer and SkyKick acknowledge that Customer will be accessing the Services as a data "controller", or any similar designation by Data Protection Law, for its own purposes. SkyKick will be the data "processor", or any similar designation by Data Protection Law, for Customer with respect to the Customer Data.

2. DATA PROCESSING AND PROTECTION

2.1. **Limitations on Use.** SkyKick will Process Personal Data only: (a) in a manner consistent with documented instructions from Customer, which will include Processing (i) to provide the Services, (ii) as authorized or permitted under the Agreement, including, where applicable, as specified in **Attachment 3** to this DPA, and (iii) consistent with other reasonable documented instructions of Customer; and (b) where allowed under Data Protection Law as required by applicable law, provided that SkyKick will inform Customer (unless prohibited by such applicable law) of the applicable legal requirement before Processing pursuant to such applicable law.

2.2. **Customer Obligations**. Customer will not instruct SkyKick to perform any Processing of Personal Data that violates any Data Protection Law. Customer represents and warrants that (i) any Personal Data provided to SkyKick is collected or otherwise Processed by Customer in accordance with Data Protection Law; (ii) any Processing of Personal Data by SkyKick performed in accordance with the Agreement does not and will not violate any Data Protection Law; and (iii) all individuals whose Personal Data is Processed by SkyKick have been notified of SkyKick's data Processing pursuant to the Services and as detailed in this DPA. SkyKick may suspend Processing based upon any Customer instructions that SkyKick reasonably suspects violate Data Protection Law. SkyKick shall inform Customer if, in SkyKick's opinion, instructions given by the Customer infringe Data Protection Law. Customer is solely responsible for the accuracy, quality, and legality of the Personal Data and the means by which Customer acquired the Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Law.

2.3. **Confidentiality.** SkyKick will ensure that any persons authorized by SkyKick to Process any Personal Data are subject to and have committed themselves to appropriate confidentiality obligations.

2.4. **Security.** SkyKick will protect Personal Data in accordance with requirements under Data Protection Law, including by implementing appropriate administrative, physical, technical and organizational safeguards as set out in **Attachment 4** to this DPA to (a) avoid accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed unauthorized or unlawful Processing of Personal Data and accidental loss, destruction of or damage to Personal Data; and (b) ensure the security of Personal Data appropriate to the risk of SkyKick's Processing under the Agreement. This in accordance with industry best practices and industry-recognized standards.

3. RETURN OR DELETION.

Upon any expiration or termination of the Agreement for any reason, and/or after the end of the provision of the Services: (a) SkyKick will delete all Personal Data, unless (i) instructed otherwise by Customer (directly or via the SkyKick Partner), or (ii) any law to which SkyKick is subject requires the continued storage of such Personal Data by SkyKick in accordance with Data Protection Law; (b) SkyKick reserves the right to delete all Personal Data retrieved or received by SkyKick, including, but not limited to, Personal Data in the SkyKick Platform, in connection with a Backup or Migration Order; and (c) Personal Data retrieved or received by SkyKick in connection with a Cloud Manager Order is retained only while there is an active connection to Customer's environment, and automatically deleted and purged when the connection to the applicable Provider Offering is removed.

Notwithstanding the foregoing, SkyKick may retain Personal Data pursuant to a lawful subpoena or court order.

Except in the case of Personal Data retrieved or received in connection with Cloud Manager, SkyKick will use commercially reasonable efforts to inform Customer (directly or via the SkyKick Partner) prior to deleting Personal Data by means of a banner in the Customer Self-Service portal or via other channels.

4. DATA PROCESSING ASSISTANCE

4.1. **Data Subject's Rights Assistance.** Taking into account the nature of the Processing of Personal Data by SkyKick under the Agreement, SkyKick will provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as possible and as necessary, for the fulfilment of the obligations of Customer to respond to requests for exercising Data Subject's rights under Data Protection Law with respect to Personal Data solely to the extent Customer does not have the ability to address such Data Subject request without such assistance.

4.2. **Data Protection Impact Assessment Assistance**. Taking into account the nature of SkyKick's Processing of Personal Data and the information available to SkyKick, SkyKick will provide reasonable assistance to Customer if required for Customer to comply with data protection impact assessment and consultation obligations (or similar obligations) as may be required by Data Protection Law in connection with SkyKick's Processing of Personal Data under the Agreement.

4.3. **Personal Data Breach Notice and Assistance.** SkyKick will notify Customer (directly or via the SkyKick Partner) without undue delay after becoming aware of a Personal Data Breach. Taking into account the nature of Processing and the information available to SkyKick, SkyKick will provide reasonable assistance to Customer as may be necessary for Customer to satisfy any notification obligations required under Data Protection Law related to any Personal Data Breach. Customer, however, has the sole right and obligation to determine whether, at its sole cost and expense, to provide notice of the Personal Data Breach to any affected Data Subjects, regulators, law enforcement agencies, third parties or others, including whether to offer any type of remedy to affected Data Subjects

5. AUDITS.

At least at two yearly intervals, SkyKick shall make available to Customer a written audit report demonstrating the former's compliance with the Data Protection Law and this DPA. If an audit report submitted by SkyKick in accordance with the above in Customer's opinion – acting reasonably – is insufficient to demonstrate compliance with the Data Protection Law and this DPA, SkyKick shall permit Customer or an independent, qualified third party appointed by Customer (each an "**Auditing Entity**"), subject to reasonable prior written notice of at least sixty (60) business days, to access to its premises, computer and other information systems, records, documents and agreements as reasonably required by the Auditing Entity to check that SkyKick is complying with its obligations under the Data Protection Law and this DPA. Any review in accordance with this paragraph 5 (i) shall not take place more than once in every twelve (12) month period and may not exceed 5 days; and (ii) shall not require the review of any third-party (including other SkyKick customers) data or the confidential information of SkyKick. Prior to a review, the Auditing Entity shall enter into such (additional) confidentiality obligations with SkyKick as may be reasonably necessary to respect the confidentiality of SkyKick's business interests and the rights and interests of any affected third parties. The Auditing Entity shall perform any audit during normal business hours only, and shall take due care during the audit not to disturb SkyKick's business operations and operational workflows. In the event that the audit leads to a delay in the provision of the Services, Customer and SkyKick will enter into discussions to resolve the matter as soon as possible. SkyKick's costs relating to any audit by an Auditing Entity shall be borne by Customer. The foregoing limitations do not apply where applicable Data Protection Law prohibits this, if Customer requests an audit following a Personal Data Breach caused by an act or omission from SkyKick, or to audits required or undertaken by a competent authority or pursuant to an enforceable court order.

6. SUBPROCESSORS

Customer authorizes SkyKick to use subcontractors to Process Personal Data in connection with the provision of Services to Customer ("**Subprocessor**"). As of the effective date of this DPA, the current list of Subprocessors is specified in **Attachment 3**. SkyKick will provide Customer (directly or via the SkyKick Partner) with notice of any intended changes concerning the addition or replacement of its Subprocessors, and provide Customer with the opportunity to object to such changes. If Customer does not object within thirty (30) days, Customer is deemed to have consented to the proposed addition or replacement. If Customer objects to any Subprocessor, SkyKick may terminate the Agreement immediately upon notice to Customer without liability. SkyKick will impose data protection obligations upon any Subprocessor that are no less protective than those included in this DPA and SkyKick shall remain liable to Customer for any breach of the obligations in this DPA by a Subprocessor in accordance with the relevant provisions in the Terms and Conditions.

7. DATA TRANSFERS

SkyKick will abide by the requirements of Data Protection Law (if any) regarding the cross-border transfer of Personal Data, including entering into such additional contractual arrangements or taking such additional measures as may be required by Data Protection Law. If Customer is

based outside the United States of America, the EEA (as defined below), and Switzerland, the SCCs (Module 4; processor-to-controller) apply. The governing law to the SCCs is Dutch law and the competent court is the Amsterdam District Court following proceedings in English before the Chamber for International Commercial Matters ("Netherlands Commercial Court" or "NCC District Court"), to the exclusion of the jurisdiction of any other courts. An action for interim measures, including protective measures, available under Dutch law may be brought in the NCC District Court in Summary Proceedings (CSP) in proceedings in English. Any appeals against NCC or CSP judgments will be submitted to the Amsterdam Court of Appeal's Chamber for International Commercial Matters ("Netherlands Commercial Court of Appeal" or "NCCA"). The NCC Rules of Procedure apply. Clause 7 and the optional language of clause 11a of the SCCs do not apply. The information for Annex IA of the SCCs is set out in the Agreement (i.e. the Parties). The information for Annex IB of the SCCs, is set out in **Attachment 3**.

In addition, SkyKick has certified compliance under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Principles, and the commitments they entail. In light of the judgement of the Court of Justice of the EU in Case C-311/18 (*Schrems II*), SkyKick no longer relies on the EU-U.S. or Swiss-U.S. Privacy Shield Framework as a legal basis for transfers or safeguard of Personal Data from the EU or Switzerland to the U.S. Customer authorizes SkyKick to provide a summary or a representative copy of the relevant privacy provisions of this DPA to the a competent authority if requested.

8. MISCELLANEOUS

8.1. **Customer Affiliates**. To the extent SkyKick Processes Personal Data on behalf of Customer's Affiliates, Customer enters into this DPA on behalf of itself and as agent for its Affiliates, and references to Customer under this DPA shall include Customer and its Affiliates; provided however that the Customer is the sole entity that may enforce this DPA on its own behalf and on behalf of its Affiliates.

8.2. **General**. This DPA forms part of the Agreement. The terms and provisions of the Agreement remain unchanged and in full force and effect. Except as otherwise stated herein, the Terms and Conditions apply to this DPA, including without limitation, any clauses set forth in the Terms and Conditions pertaining to limitation of liability. This DPA will automatically terminate upon the termination or expiration of the Agreement except as otherwise stated herein. SkyKick may from time to time amend this DPA in accordance with clause 13.10 of the Terms and Conditions, unless and to the extent applicable law requires otherwise. This DPA shall be governed by and construed in accordance with the laws applicable to the Terms and Conditions. All disputes that may arise out of or in connection with this DPA, or with any agreement, document, or instrument entered into pursuant hereto or in furtherance hereof, shall be brought exclusively before the competent court according to the Terms and Conditions.

8.3. **Execution**. This DPA will be executed electronically as part of the Terms and Conditions. This DPA will be effective as of the date that Customer accepts (directly or via the SkyKick Partner) the Terms and Conditions.

LOCAL PROVISIONS NORTH AMERICA

9. **United States.** If the Customer is based in the United States, the following applies in addition to the remainder of this DPA:

9.1 This DPA is with SkyKick LLC.

9.2 **Terms**. The following capitalized terms have the meanings set forth below:

9.2.1 "**Business Purpose**", "**Sell**", and "**Service Provider**" have the definitions ascribed to them in the CCPA.

9.2.2 "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended or replaced from time to time, and any regulations implementing the foregoing.

9.2.3 "**Personal Data**" means any data that SkyKick Processes via the Services on behalf of Customer that relates to a Data Subject, including, but not limited to, any information that meets the definition of "personal information" under the CCPA.

9.2.4 "**Share**" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

9.3 **CCPA Requirements**. The Parties acknowledge and agree that, to the extent Personal Data contains any data regulated by the CCPA, the applicable Business Purposes are the Services described in the Agreement, including this DPA (collectively, the "**Specified Business Purpose**") and SkyKick certifies, as a Service Provider to Customer, that it understands, and will comply with, the applicable restrictions set forth in the CCPA and that:

9.3.1 SkyKick shall Process all Personal Data on behalf of Customer only;

9.3.2 SkyKick is prohibited from retaining, using, or disclosing Personal Data for any purpose other than for the Specified Business Purpose, including, without limitation, from retaining, using, or disclosing such Personal Data (A) for a purpose other than the Specified Business Purpose, or (B) outside of the direct business relationship between the relevant Data Subject and the Customer (and SkyKick on behalf of Customer);

9.3.3 SkyKick shall not further collect, use, or disclose Personal Data except as necessary to provide the Services;

9.3.4 SkyKick shall not Sell or Share the Personal Data for any reason;

9.3.5 SkyKick shall not, unless otherwise explicitly permitted by applicable law, combine Personal Data with other personally identifiable information it (A) receives from or on behalf of another person or third party, or (B) collects from its own interactions with the applicable Data Subject;

9.3.6 SkyKick shall notify Customer as soon as practical if SkyKick determines it can no longer meet any of its obligations under this clause 13.2;

9.3.7 If Customer believes SkyKick is collecting, using, Processing, or sharing Personal Data in a manner inconsistent with the Agreement (an "**Unauthorized Use**"), then SkyKick shall, upon receiving written or oral notice from Customer, cease all collection, use, Processing, or sharing of Customer Data as soon as practical; and

9.3.8 SkyKick shall provide Customer with reasonable assistance and work with Customer in good faith in order to fully resolve and remediate the Unauthorized Use.

10. **Canada.** If the Customer is based in Canada, the following applies in addition to the remainder of this DPA:

10.1 This DPA is with SkyKick B.V.

10.2 **"Data Protection Law**" shall be taken to include, where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

10.3 The Customer shall, in accordance with Data Protection Law, give any required notices and obtain any required consents from Data Subjects, including any such notice or consent required for the cross-border transfer of Personal Data for Processing.

10.4 The Customer will provide SkyKick with all the guidance and reasonable assistance needed for SkyKick to meet its obligations under Data Protection Law.

10.5 SkyKick may disclose or provide access to Personal Data to a Canadian enforcement, surveillance, other governmental authority, court or tribunal (each a "**Competent Authority**") if it is subject to a request to disclose or provide access to Personal Data by a Competent Authority.

LOCAL PROVISIONS EU/EEA, UK & SWITZERLAND

11. **European Union / European Economic Area** ("**EEA**"). If the Customer is based in the European Union or the EEA, the following applies in addition to the remainder of this DPA:

11.1 This DPA is with SkyKick B.V.

11.2 Personal Data may be transferred to, and stored and Processed by, Subprocessors located outside the EEA. Any Personal Data transferred from SkyKick to a Subprocessor located outside the EEA shall be governed by the SCCs (Module 3; processor-to-processor), executed between SkyKick and the relevant Subprocessor, unless the Subprocessor is established in a country for which the European Commission adopted an adequacy decision.

11.3 If there is any conflict between the terms of any SCCs or other contractual arrangements required by Data Protection Law, as the case may be, in force under this DPA and any terms of this DPA (or other terms and conditions as may be imposed from time to time), the terms of the SCCs or the other contractual arrangements required by Data Protection Law shall prevail.

12. **United Kingdom.** If the Customer is based in the United Kingdom, then the following applies in addition to the remainder of this DPA:

12.1 This DPA is with SkyKick B.V.

12.2 “Personal Data” will be taken to include Business Contact Data.

12.3 Personal Data may be transferred to, and stored and Processed by, Subprocessors located outside the United Kingdom. Any Personal Data transferred from SkyKick to a Subprocessor located outside the United Kingdom shall be governed by the SCCs (Module 3; processor-to-processor) as amended by the United Kingdom’s International Data Transfer Addendum to the European Commission’s standard Contractual Clauses (or any replacement international data transfer agreement adopted by the UK Government from time to time) (the “**UK SCCs**”), entered between SkyKick and the relevant Subprocessor, as a data importer, unless the Subprocessor is established in a country for which the United Kingdom adopted an adequacy decision.

13. **Switzerland**. If Swiss data protection law applies to the processing of personal data by SkyKick, the following applies in addition to the remainder of this DPA:

13.1 This DPA is with SkyKick B.V.

13.2 Personal Data may be transferred to, and stored and processed by Subprocessors located outside Switzerland. Any Personal Data transferred from SkyKick to a Subprocessor located outside Switzerland shall be governed by the Standard Contractual Clauses adopted pursuant to SCCs (Module 3; processor-to-processor), taking into account the necessary measures and contractual modifications from the perspective of Swiss law according to the current state of doctrine and practice, entered between SkyKick and the relevant Subprocessor, unless the Subprocessor is established a country for which Switzerland adopted an adequacy decision.

13.3 The notice period for audits in section 5 of this DPA shall be replaced by a notice period of ten (10) business days. Until the entry into force of the revised Swiss data protection law, data of legal persons are also considered Personal Data within the meaning of this DPA.

LOCAL PROVISIONS ASIA-PACIFIC & SOUTH AFRICA

14. **Australia.** If the Customer is based in Australia, the following applies in addition to the remainder of this DPA:

14.1 This DPA is with SkyKick B.V.

14.2 “Personal Data” will be taken to include Business Contact Data to the extent that it relates to a Data Subject.

14.3 Without prejudice to clause 4.3 of this DPA, Customer will notify SkyKick without undue delay after becoming aware of a Personal Data Breach. Taking into account the nature of Processing and the information available to Customer, Customer will provide reasonable assistance to SkyKick as may be necessary for SkyKick to satisfy any assessment or notification obligations required under Data Protection Law related to any Personal Data Breach.

14.4 Customer will provide SkyKick with all the guidance and reasonable assistance needed for SkyKick to meet its obligations under Data Protection Law.

14.5 SkyKick may disclose or provide access to Personal Data to an Australian enforcement, surveillance, other governmental authority, court or tribunal (each a “**Competent Authority**”) if it is subject to a request to disclose or provide access to Personal Data by a Competent Authority.

14.6 Customer will cooperate with SkyKick to provide any information which SkyKick may reasonably request in order to assist SkyKick comply with the Security of Critical Infrastructure Act 2018 (Cth) as amended from time to time.

15. **Japan.** If the Customer is based in Japan, the following applies in addition to the remainder of this DPA:

15.1 This DPA is with SkyKick B.V.

15.2 Personal Data may be transferred to, and stored and Processed by, Subprocessors located outside Japan in compliance with the Act on Protection of Personal Information (“**APPI**”).

15.3 The Customer shall obtain consent from a Data Subject to transfer Personal Data to the United States in accordance with APPI.

15.4 If any of the technical and organizational security measures set out in **Attachment 4** is changed, SkyKick shall inform Customer of the change(s) without undue delay.

15.5 With regard to clause 5 of this DPA, SkyKick shall make available to Customer a written audit report demonstrating the former's compliance with the Data Protection Law and this DPA at yearly intervals.

16. **South Africa.** If the Customer is based in South Africa, the following applies in addition to the remainder of this DPA:

16.1 This DPA is with SkyKick B.V.

16.2. Definitions

16.2.1 "**Applicable Data Protection Laws**" means Protection of Personal Information Act, No. 4 of 2013, Electronic Communications and Transactions Act No. 25 of 2002, Promotion of Access to Information Act No. 2 of 2000, Regulation of Interception of Communications and Provision of Communication Related Information Act No. 70 of 2002, Consumer Protection Act No. 68 of 2008 and any regulations published under it read in conjunction with any other Applicable Laws as the case may be as well as any in-country equivalent legislation;

16.2.2 "**Data Subject**" means the Customer, and its customers, suppliers, subcontractors, subprocessors and employees;

16.2.3 "**Information Officer**" means the Customer's Information Officer;

16.2.4 "**Operator**" means SkyKick B.V. who processes Personal Information for the Customer in terms of this DPA, without coming under the direct authority of the Customer;

16.2.5 "**Personal Information**" means Personal Data, relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including;

16.2.6 "**Regulator**" means the Information Regulator who is the authority for enforcement as defined in Applicable Data Protection Laws;

16.2.7 "**Responsible Party**" means the Customer who, alone or in conjunction with others, determines the purpose of and means for processing Personal Data;

16.2.8 "**Special Personal Information**" means the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of the Data Subject; or the criminal behavior of a Data Subject to the extent that such information relates to:

- the alleged commission by a Data Subject of any offence; or
- any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

16.3. Processing of special personal information

16.3.1. The Operator shall not Process the Special Personal Information of Data Subjects unless:

- Processing is carried out with the consent of the Data Subject;
- Processing is necessary for the defence of a right or obligation in law;
- Processing is for historical, statistical or research purposes which purpose serves as a public interest or it appears to be impossible to ask for consent;
- Information has deliberately been made public by the Data Subject; and
- The provisions of section 28 to 33 of POPIA have been complied with.

16.4. Disclosure or processing required by law, regulation or court order

16.4.1. In the event that Operator is required to disclose or Process any Personal Data of a Data Subject in terms of a legally binding request for disclosure or court order, Operator:

- will advise the Customer thereof prior to disclosure, if possible and legally permissible. If prior disclosure is not possible, the Operator shall advise the Customer immediately after such disclosure unless otherwise prohibited such as a prohibition in terms of criminal law to preserve confidentiality of an investigation by a law enforcement agency;
- will take such steps to limit the extent of the disclosure or Processing insofar as it reasonably practically and legally allowable;
- will afford the Customer a reasonable opportunity, if possible and legally permitted, to intervene in the proceedings; and
- will comply with the Customer's requests as to the manner and terms of any such disclosure or Processing, if possible and legally permitted.

16.5. Transfer of personal information

16.5.1. Skykick shall ensure that no Personal Information of Data Subjects is transferred outside of the Republic of South Africa unless:

- the Customer provides its prior written consent to the transfer;
    - the recipient is subject to a law, code of conduct or contract which provides comparable protection for the Personal Information as the protections contained in this clause 16, including similar provisions relating to the further transfer of the Personal Information;
    - the transfer is necessary for the performance of a contract between the Data Subject and the Customer, or a contract between the Customer and Operator which is in the interest of the Data Subject; or
    - the transfer is for the benefit of the Data Subject and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.

***

Attachment 1: Definitions

For purposes of this DPA, the following terms will have the meaning ascribed below:

"**Affiliate**" means, as to any entity, any other entity that, directly or indirectly, Controls, is Controlled by or is under common Control with such entity.

"**Control**" for the purposes of this clause will mean with respect to any person or entity, the right to exercise or cause the exercise of at least fifty per cent (50%) or more of the voting rights in such person or entity.

"**Agreement**" has the meaning ascribed to in the Terms and Conditions.

"**Business Contact Data**" means information relating to any individual that uses the Services on behalf of Customer, which may include name, email address and other contact information.

"**Data Protection Law**" means any and all privacy, security, or data protection laws and regulations that apply to the Processing of Personal Data by SkyKick under the Agreement.

"**Data Subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Personal Data**" means any data that SkyKick Processes via the Services on behalf of Customer that relates to a Data Subject. Personal Data does not include Business Contact Data, unless Data Protection Law stipulates otherwise.

"**Personal Data Breach**" means (i) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, or (ii) a data breach or similar event as defined by the relevant Data Protection Law.

"**Process**" or "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Services**" means the services provided by or on behalf of SkyKick pursuant to the Agreement.

"**SkyKick Partner**" means the service provider from whom the Customer has procured the Services.

"**SCCs**" means the standard contractual clauses as adopted pursuant to European Commission's decision (EU) 2021/914.

"**Terms and Conditions**" means the SkyKick Customer terms and conditions that apply to the Services and in which this DPA is referenced.

***

Attachment 2 – Data Pro Statement

Along with the DPA and its Attachments this Data Pro Statement constitutes the DPA for the product or service(s) as provided by the company that has drawn up this Data Pro Statement for Customers located outside the United States of America.

General information

1. Data Processor

This Data Pro Statement was drawn up by the following data processor:

SkyKick B.V. ("**SkyKick**")

James Wattstraat 100

1097 DM Amsterdam

The Netherlands

If you have any queries about this Data Pro Statement or data protection in general, please contact:

Gerard Doeswijk

Global Data Protection Officer

DataPrivacy@SkyKick.com

2. Effective date

The Data Pro Statement shall enter into force on 5th of November 2020

We regularly revise our security measures described in this Data Pro Statement to ensure that we are always fully prepared and up to date regarding data protection. If this document is updated, we shall notify you of the revised versions through our regular channels

3. Applicability

This Data Pro Statement applies to the following products and services as provided by SkyKick: The entirety of the SkyKick Platform, including SkyKick Migration Suites, SkyKick Cloud Backup for Office 365 & SkyKick Cloud Manager.

4. SkyKick Product Descriptions

4.1 SkyKick Migration Suites

With the SkyKick cloud migration resellers can assist customers with cloud migration projects from pre-sales to project completion. Further product information is available here:

https://www.skykick.com/migrate/

4.2 SkyKick Cloud Backup

The SkyKick cloud backup solution allows customers to protect their data from ransomware and other malicious and indeliberate events which lead to data loss or data corruption. Further product information is available here:

https://www.skykick.com/office-365-backup/

4.3 Description of SkyKick Cloud Manager

The SkyKick cloud management product cloud allows for seamless management of services across a customer, SaaS, and even hybrid environments. Through automation customers can improve their help desk performance and strengthen security and data protection. Further product information is available here:

https://www.skykick.com/cloud-management/

5. Intended use of the SkyKick Services

The SkyKick platform was designed and built to process the types of data as described in **Attachment 3** – Scope of Processing. When the services were designed the possibility that these would be used to process special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government was not considered. It is up to Customer to determine whether it shall use the SkyKick services to process such data.

6. Processing of data outside the EU/EEA.

SkyKick has ensured that the personal data shall be protected to an appropriate standard as any personal data transferred from SkyKick to a Subprocessor located outside the EEA, United Kingdom and Switzerland) shall be governed by the Standard Contractual Clauses Module 3 (processor-to-processor), entered between SkyKick and the relevant Subprocessor.

As part of its commitment to the adherence to GDPR and Swiss Data Protection Law SkyKick can – on entering into a non-disclosure agreement with the customer – provide additional detail on the additional safeguards it has put in place to complement the Standard Contractual Clauses to ensure its compliance with the GDPR and Swiss Data Protection Law in light of recent ruling from the EU Court of Justice in the case Schrems II.

7. Use of sub processors:

All current sub processors of SkyKick are listed in **Attachment 3** – Scope of Processing section 3.

8. Support with requests from Data Subjects:

SkyKick shall support its Customers to respond to requests from Data Subjects as described in the DPA section 4.1

9. Support with Data Privacy Impact Assessments (DPIA)

SkyKick shall support its Customers with Data Privacy Impact Assessments (DPIA) as described in the DPA section 4.2

10. Data deletion

Upon any expiration or termination of the Agreement with a Customer for any reason, SkyKick shall delete personal data it processes on behalf of Customer in such a manner that they shall no longer be able to be used and shall be rendered inaccessible and as further described in the DPA section 3.

Further details on the deletion of data and the automation can be provided upon request through our Global Data Protection Officer (see contact details above).

11. Data exports

If desired by a customer, once an agreement with a customer has been terminated SkyKick can return personal data it processes, as further described in the DPA section 3.

Security policy

SkyKick has implemented the security measures as described in **Attachment 4** – Technical & Organization Security Measures. And SkyKick adheres to the core principles of the following frameworks in relation to the maintenance of its Information Security Management System (ISMS):

- NEN-ISO 9001
- NEN-ISO 27001
- Microsoft Security Development Lifecycle
- CAIQ V3.1

SkyKick has obtained the following certificates

- Data Pro+ Certificate
- ISO 27001:2013

Data leak protocol

In the unfortunate event something does go wrong, SkyKick shall follow the data breach protocol as described in the DPA section 4.3. If Customer is based in Australia, section 9 shall apply in addition to section 4.3.

***

Attachment 3 – Scope of Processing

1. Subject-Matter and Duration of Processing

SkyKick B.V. Processes Personal Data for the subject matter specified under the Agreement and until the Agreement terminates or expires, unless otherwise agreed upon by the parties in writing. In particular, the subject matter is determined by the Services to which Customer subscribes.

2. Nature and Purpose of Processing

The nature of the Processing is cloud migration, cloud storage and cloud management. A more detailed description of the nature and purposes of the Services can be made available upon request in accordance with applicable law and the Agreement.

3. Subcontractor's Processing of Personal Data

In the below table is a summary of the categories of data, and storage locations for SkyKick B.V.'s current Subprocessors and their respective Processing activities.

Subprocessor	**Scope and purpose of processing**	**Categories of Personal Data**	**Processing (and storage) locations (e.g. country/state)**
SkyKick LLC (200 West Thomas Street, Seattle, WA98119 USA)	Provision of (technical) support	Personal data as described under Section 4 below	United States

The duration of processing is the term of the distribution and services agreement between SkyKick B.V. and SkyKick LLC. The subject matter and nature of the processing is access to Personal Data for support services under the distribution and services agreement between SkyKick B.V. and SkyKick LLC.

4. Types of Personal Data

Categories of Personal Data to be processed under this DPA includes the following categories of data: names, e-mail addresses and other contact details, as well as any personal data that may be included in the content of e-mails. More specifically:

	Migrations	Backup	Manager
Administrator accounts [1]			
Username	√		
Password	√ [2]		
User accounts			
Username	√	√	√
Password	√ [3]		
Email address	√	√	√
First name	√	√	√
Last name	√	√	√
Job title	√	√	√
Business phone	√	√	√
Employee number			√

Department	√
Location	√

DNS Registrar credentials

Username	√
Password	√

[1] For SkyKick Cloud Backup & Cloud Manager multi-factor authentication is used, no usernames or passwords are stored and access to the underlying SAAS service is granted based on an authentication token.

[2] SkyKick recommends using a temporary administrator account for migrations which should be disabled on the completion of the migration.

[3] May be applied to obtain access to the source for the migration if this access cannot be obtained through the administrator account. SkyKick in all cases recommends resetting the password on the destination environment on completion of a migration and provides automation to support this.

5. Categories of Data Subjects

The categories of Data Subjects are Customer employees, contractors, business partners and other individuals whose Personal Data is included in the Customer Data. If Customer is based in South Africa, juristic persons are also included.

6. The frequency of the Processing (e.g. whether the data is processed on a one-off or continuous basis).

The frequency of the Processing is on a continuous basis.

***

Attachment 4 – Technical & Organizational Security Measures

SkyKick has various technical and organizational security measures in a place to secure, maintain and safeguard Personal Data. The security commitments in this DPA are the sole responsibility of SkyKick with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. SkyKick has appointed a data protection team responsible for coordinating, monitoring and regularly auditing all rules and procedures. **Security Roles and Responsibilities**. SkyKick staff with access to Personal Data are subject to confidentiality obligations. **Risk Management Program**. SkyKick performed a risk assessment before processing Personal Data through their Services and retains related documents pursuant to applicable retention requirements.
Asset Management	**Asset Inventory**. SkyKick maintains an inventory of all media on which Personal Data is stored. Access to the inventories of such media is restricted to SkyKick employees authorized to have such access. **Asset Handling** SkyKick classifies Personal Data to help identify it and to allow for access to it to be appropriately restricted. SkyKick imposes restrictions on printing Personal Data and has procedures for disposing of printed materials that contain Customer Data.

	SkyKick staff must obtain SkyKick authorization prior to storing Personal Data on portable devices, remotely accessing Customer Data, or processing Personal Data outside SkyKick's facilities.
Human Resources Security	**Security Training**. SkyKick informs its staff about relevant security procedures and their respective roles. SkyKick also informs its staff of possible consequences of breaching the security rules and procedures. SkyKick will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. SkyKick limits access to facilities where information systems that process Personal Data are located to identified authorized staff members. **Physical Access to Components**. Where applicable, SkyKick maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Personal Data they contain. **Protection from Disruptions**. SkyKick applies a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. SkyKick uses industry standard processes to delete Personal Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. SkyKick maintains security documents describing its security measures and the relevant procedures and responsibilities of its staff who have access to Customer Data. **Data Recovery Procedures** On an ongoing basis SkyKick maintains copies of Personal Data from which Personal Data can be recovered. SkyKick stores copies of Personal Data and data recovery procedures in a different container from where the processing the Personal Data is performed. SkyKick has procedures in place governing access to copies of Customer Data. SkyKick reviews its data recovery procedures at least annually. SkyKick logs data restoration efforts, including the person responsible, the description of the restored data and where applicable and the person responsible. **Malicious Software**.

SkyKick has anti-malware controls to help avoid malicious software, including malicious software originating from public networks, gaining unauthorized access to Customer Data.

Data Beyond Boundaries

SkyKick encrypts, or enables Customer to encrypt, Personal Data that is transmitted over public networks.

SkyKick restricts access to Personal Data in media leaving its facilities.

Event Logging.

SkyKick logs the access and use of information systems containing Customer Data, registering the user ID, time, authorization granted or denied, and relevant activity of its staff members.

Access Control

Access Policy.

SkyKick maintains a record of security privileges of staff members having access to Customer Data.

Access Authorization

SkyKick maintains and updates a record of staff authorized to access SkyKick systems that contain Customer Data.

SkyKick deactivates authentication credentials that are not used for a period not exceeding six months.

SkyKick identifies those staff members who may grant, alter or cancel authorized access to data and resources.

SkyKick ensures that where more than one individual has access to systems containing Customer Data, the staff members have separate user identifiers and log-ins.

Least Privilege

SkyKick staff members are only permitted to have access to Personal Data when required.

SkyKick restricts access to Personal Data to only those staff members who require such access to perform their job function.

Integrity and Confidentiality

SkyKick instructs SkyKick staff to disable administrative sessions when leaving premises SkyKick controls or when computers are otherwise left unattended.

SkyKick stores passwords in a way that makes them unintelligible while they are in force.

Authentication

SkyKick uses industry standard practices to identify and authenticate users who attempt to access information systems.

Where authentication mechanisms are solely based on passwords, SkyKick requires that the passwords are renewed regularly.

Where authentication mechanisms are solely based on passwords, SkyKick requires the password to be at least eight characters long.

SkyKick ensures that de-activated or expired identifiers are not granted to other staff members.

SkyKick monitors repeated attempts to gain access to the information system using an invalid password.

SkyKick maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

SkyKick uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network Design.

SkyKick has controls to avoid staff members assuming access rights they have not been assigned to gain access to Personal Data they are not authorized to access.

Information Security Incident Management

Incident Response Process

SkyKick maintains a record of security incidents with a description of the incident, the time period, its consequences, the name of the reporter, and to whom the incident was reported, and the procedure for recovering from an incident.

For each incident pertaining to Customer Data, notification by SkyKick will be made without undue delay and, in any event, within 72 hours.

SkyKick tracks disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.

Service Monitoring.

SkyKick security staff verify logs at least every six months to propose remediation efforts if necessary.

Business Continuity Management

SkyKick maintains emergency and contingency plans for the facilities in which SkyKick information systems that process Personal Data are located.

SkyKick's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original or last-replicated state from before the time it was lost or destroyed.

***