DATA PROCESSING ADDENDUM

1. **Applicability.**
   This Data Processing Addendum ("**DPA**") shall apply to the services agreement ("**Services Agreement**") by and between SafeBreach Inc. and its affiliates ("**SafeBreach**") and you ("**Client**") to the extent that SafeBreach processes Personal Data (as defined below).

2. **Definitions.**
   2.1. Terms used in this DPA but not defined herein (whether or not capitalized) shall have the meanings assigned to such terms in the Applicable Data Protection Laws.
   2.2. "**Applicable Data Protection Laws**" shall mean, to the extent applicable to SafeBreach's processing of Personal Data hereunder (with respect to each data subject): (i) General Data Protection Regulations (European Parliament and Council of European Union (2016) Regulation (EU) 2016/679) (EU GDPR); (ii) EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 and UK Data Protection Act 2018 (UK GDPR) ; (iii) California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA); (iv) Protection of Privacy Law (Israel); and (v) any rules or regulations that amend and/or replace any of the aforementioned Data Protection Laws.
   2.3. "**Personal Data**" refers to the definition of that term or any other similar term defined under the Applicable Data Protection Laws.
   2.4. "**Services**" means the services provided by SafeBreach to Client in accordance with the Terms (as defined below).
   2.5. "**Standard Contractual Clauses or SCCs**" shall mean: where the EU GDPR applies, the standard contractual clauses pursuant to the EU Commission's Implementing Decision 2021/914 of 4 June 2021 currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj ("**EU SCCs**"); (ii) where the UK GDPR applies, the EU SCCs together with the UK Information Commissioner's Office addendum, under S119A(1) of the Data Protection Act 2018 ("**UK Addendum**"); or any other Standard Contractual Clauses which amended and/or replace such Standard Contractual Clauses in accordance with Applicable Data Protection Law.

3. **Processing of Personal Data on behalf of Client.**
   SafeBreach acts as a processor/service provider for Client, and performs processing operations on behalf of Client and upon the instructions of Client as a controller/business, as set forth herein, in the Services Agreement, and any additional agreement entered into between Client and SafeBreach (collectively, the "**Terms**"), pursuant to which Client may provide Personal Data to SafeBreach ("**Contracted Business Purpose**").

4. **Client Representations.**
   Client sets forth the details, including the purpose, the means and the ways in which SafeBreach shall process Personal Data, as required by Applicable Data Protection Laws in **Appendix A** (*Details of Processing of Processed Personal Data*), attached hereto, and Client represents and warrants that:

4.1. It complies with personal data security and other obligations prescribed by Applicable Data Protection Laws for controller/business, and that the provision of Personal Data to SafeBreach is in strict compliance with Applicable Data Protection Laws;

4.2. It only processes Personal Data that has been collected in accordance with the Applicable Data Protection Laws;

4.3. It has in place procedures in case an individual whose Personal Data is collected, wish to exercise their rights in accordance with the Applicable Data Protection Laws;

4.4. It provides Personal Data to SafeBreach for the Contracted Business Purpose in accordance with the representations Client makes to individuals in Client's privacy policy, and Client does not sell Personal Data to SafeBreach;

4.5. It shall provide to SafeBreach as a processor/service provider, or otherwise have SafeBreach (or anyone on its behalf) process such Personal Data which is explicitly permitted under Applicable Data Protection Laws ("**Permitted Personal Data**"). Solely Client shall be liable for any data which is made available to SafeBreach in excess of the Permitted Personal Data ("**Non-Permitted Data**"). SafeBreach's obligations under the Terms shall not apply to any such Non-Permitted Data;

4.6. It is and will remain duly and effectively authorized to give the instruction set out herein and any additional instructions as provided pursuant to the Terms, at all relevant times and at least for as long as the Terms are in effect and for any additional period during which SafeBreach is lawfully processing Personal Data.

5. SafeBreach Obligations.

5.1. SafeBreach carries out the processing of Personal Data on Client's behalf;

5.2. Pursuant to the provisions of Article 28 of the GDPR, to the extent applicable with respect to each data subject, SafeBreach agrees that it will:

5.2.1. process Personal Data solely on Client's behalf and in compliance with Client's instructions, including instructions in this DPA and all Terms, unless required to do so by EU or applicable Member State law;

5.2.2. implement appropriate technical and organizational measures to provide an appropriate level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR;

5.2.3. take reasonable steps to ensure that access to the processed Personal Data is limited on a need to know/access basis, and that all SafeBreach personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Personal Data;

5.2.4. it shall provide reasonable assistance to Client with any data protection impact assessments or prior consultations with supervising authorities in relation to processing of Personal Data by the processor/service provider, as required under any Applicable Data Protection Laws, at the written request of the Client, and at Client's sole expense; and

5.3. Pursuant to the CCPA, to the extent applicable with respect to each data subject, SafeBreach agrees that:

5.3.1. SafeBreach is acting solely as a service provider with respect to Personal Data;

5.3.2. SafeBreach shall not retain, use or disclose Personal Data for any purpose other than for the Contracted Business Purpose;

5.3.3. SafeBreach may de-identify or aggregate Personal Data as part of performing the Services specified in the Terms; and

5.3.4. SafeBreach will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible operational purpose.

6. **Sub-Processing.**

6.1. Client authorizes SafeBreach to appoint sub-processors in accordance with the provision of the Terms. Any sub-processor used must qualify as a service provider under the Applicable Data Protection Laws and SafeBreach cannot make any disclosures to the subcontractor that the CCPA would treat as a sale.

6.2. SafeBreach may continue to use those sub-processors already engaged by SafeBreach as of the date of this DPA. Client acknowledges and agrees that as of the date of this DPA SafeBreach uses certain sub-processors; a list of such sub-processors is attached hereto as Appendix C.

6.3. SafeBreach may appoint new sub-processors and shall give reasonable notice of the appointment of any new sub-processor. Client's continued use of the applicable Services after such notification constitutes Client's acceptance of the new sub-processor.

7. **Data Subjects' Rights.**

7.1. Client shall be solely responsible for compliance with any statutory obligations concerning requests to exercise data subject rights under Applicable Data Protection Laws (e.g., for access, rectification, deletion of processed Personal Data, etc.). SafeBreach shall reasonably endeavor to assist Client insofar as feasible, to fulfil Client's said obligations with respect to such data subject requests, as applicable, at Client's sole expense.

7.2. SafeBreach shall (i) without undue delay notify Client if it receives a request from a data subject under any Applicable Data Protection Laws in respect of processed personal data; and (ii) not respond to that request, except on the written instructions of Client or as required by Applicable Data Protection Laws, in which case SafeBreach shall, to the extent permitted by Applicable Data Protection Laws, inform Client of that legal requirement before it responds to the request.

8. **Personal Data Breach.**

8.1. SafeBreach shall notify Client without undue delay upon SafeBreach becoming aware of any personal data breach within the meaning of Applicable Data Protection Laws relating to Personal Data which may require a notification to be made to a supervisory authority or data subject under Applicable Data Protection Laws "**Personal Data Breach**").

8.2. At the written request of the Client and at Client's sole expense, SafeBreach shall provide reasonable co-operation and assistance to Client in respect of Client's

obligations regarding the investigation of any Personal Data Breach and the notification to the supervisory authority and data subjects in respect of such a Personal Data Breach.

9. **Deletion or Return of Processed Personal Data.**
   9.1. Subject to the terms hereof, SafeBreach shall promptly and in any event within up to sixty (60) days (unless a sooner time period is required by Applicable Data Protection Laws) return and then destroy the Personal Data, except such copies as authorized including under this DPA or required to be retained in accordance with Applicable Data Protection Laws.
   9.2. SafeBreach may retain Personal Data to the extent authorized or required by Applicable Data Protection Laws, provided that SafeBreach shall ensure the confidentiality of such Personal Data and shall ensure that it is only processed for such legal purpose(s).
   9.3. Upon Client's prior written request, SafeBreach shall provide written certification to Client that it has complied with this Section 9.

10. **Audit Rights**
    10.1. Subject to the terms hereof, and not more than once in each calendar year, SafeBreach shall make available to a reputable auditor mandated by Client in coordination with SafeBreach, at the cost of the Client, upon prior written request, within normal business hours at SafeBreach premises, such information necessary and relevant to reasonably demonstrate compliance with this DPA, and shall allow for audits by such reputable auditor mandated by the Client in relation to the processing of the Personal Data by the processor/service provider, provided that such third-party auditor shall be subject to confidentiality obligations.
    10.2. Client shall use (and ensure that each of its mandated auditors use) its best efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the SafeBreach's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

11. **International Data Transfers**
    11.1. To the extent that SafeBreach transfers Personal Data to countries outside of the European Economic Area and/or outside of the United Kingdom (UK), which do not provide an adequate level of data protection, as determined by the European Commission pursuant to Article 45 of GDPR, and by the Secretary of State, pursuant to Section 17A of the United Kingdom Data Protection Act 2018, respectively, or other adequate authority as determined by the EU and the UK ("**Adequacy Decisions**"), and to the extent applicable with respect to each data subject, such transfer of Client's Personal Data to other countries, where the application of the SCCs, as between the parties, is required under Applicable Data Protection Laws shall be subject to: (i) Adequacy Decisions; (ii) exemptions under Article 49 of the GDPR; or (iii) the Standard Contractual Clauses are incorporated into this DPA by reference, which shall be implemented as follows:
    .

11.1.1. In the case of transfer of Personal Data between Client to SafeBreach, the parties shall implement Module II - "Controller to Processor", of the Standard Contractual Clauses, with modifications detailed under this Section 11.1.1, in which case SafeBreach shall be deemed as a "Data Importer" and Client shall be deemed as a "Data Exporter". The parties are deemed to have accepted and executed the SCCs, including the associated annexes. The contents of Annex I of the SCCs are included within Appendix A to this DPA. The contents of Annex II of the SCCs are included within Appendix B to this DPA. The parties further agree to the following implementation choices under the SCCs:

11.1.1.1. The Parties agree that for the purpose of transfer of Personal Data between SafeBreach (Data Importer) and the Client (Data Exporter), the following shall apply:

11.1.1.2. Clause 7: shall not be applicable.

11.1.1.3. Clause 9(a): The parties choose Option 2, "General Written Authorization" and specify a time period of thirty (30) days. Appendix C, shall be updated accordingly.

11.1.1.4. Clause 11: The parties choose not to include the optional language relating to the use of an independent dispute resolution body.

11.1.1.5. Clause 17: The parties select Option 1 and specify the law of Ireland.

11.1.1.6. Clause 18(b): The parties specify the courts of Ireland.

11.1.2. In the case of transfer of Personal Data between SafeBreach and its Sub-Processors for the purposes of carrying out specific Processing activities (on behalf of Client) the Partis will enter into Module III ("Processor-to-Processor") of the Standard Contractual Clauses. For the purpose of such engagement, SafeBreach shall be deemed as the Data Exporter and the Sub-Processor shall be deemed as the Data Importer; all other Modules are not applicable.

11.1.3. If the applicable Data Exporter, under Section 11.1.1 or 11.1.2, is transferring Personal Data governed by the UK GDPR, the parties agree to implement the applicable SCCs, as modified by the UK Addendum. The information required by Table 1 of the UK Transfer Addendum appears within Appendix A to this DPA. In addition, the parties adopt the SCCs, as modified by the UK Transfer Addendum, as to applicable international transfers of UK Personal Data in exactly the same manner set forth in Section 11.1 above, subject to the following:

11.1.3.1. Clause 13: The UK Information Commissioner's Office ("ICO") shall be the competent supervisory authority.

11.1.3.2. Clause 17: The SCCs, as modified by the UK Transfer Addendum, shall be governed by the laws of England and Wales.

11.1.3.3. Clause 18: The parties agree that any dispute arising from the SCCs, as modified by the UK Transfer Addendum, shall be resolved by the courts of England and Wales. A UK Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts.

11.2. Appendixes A, B, C and D, attached to this DPA shall also apply in connection with the processing of Personal Data, subject to Applicable Data Protection Law.

11.3. SafeBreach reserves the right to adopt an alternative compliance standard to the SCCs for the lawful transfer of Personal Data, provided it is recognized under Data Protection Law. SafeBreach will provide 30 days' advance notice of its adoption of an alternative compliance standard.

12. General Terms.

12.1. Governing Law and Jurisdiction. All disputes with respect to this DPA shall be determined in accordance with the governing law provisions set forth in the Services Agreement.

12.2. Conflict. In the event of any conflict or inconsistency between this DPA and any other agreements between the parties, including agreements entered into after the date of this DPA, the provisions of this DPA shall prevail.

12.3. Changes in Applicable Data Protection Laws. Client may by at least forty-five (45) calendar days' prior written notice to processor/service provider, request in writing any changes to this DPA, if they are required, as a result of any change in any Applicable Data Protection Law, regarding the lawfulness of the processing of Personal Data. If Client provides its modification request, SafeBreach shall make commercially reasonable efforts to accommodate such modification request, and Client shall not unreasonably withhold or delay agreement to any consequential changes to this DPA to protect the SafeBreach against any additional risks, and/or to indemnify and compensate SafeBreach for any further costs associated with the changes made hereunder.

12.4. Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, the parties have executed this DPA:

SafeBreach: **Client**:

_____   _____
SafeBreach Ltd.   _____
Name: _____   Name: _____
Title: _____   Title: _____

Appendix A

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: _____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: _____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

B. DETAILS OF PROCESSING OF PROCESSED PERSONAL DATA(As required by Article 28(3) of the GDPR)

1. The subject matter and duration of the processing of processed personal data are set forth in the Terms.

2. The nature and purpose of the processing of personal data is rendering the Services, as detailed and defined in the Terms.

3. The types of processed personal data to be processed are as detailed in the Services Agreement, may include:

Name, Email address, and online identifiers (such as IP address for example) of registered users (e.g., Client employees).

To the extent Client requested access to the SafeBreach Propagate offering, SafeBreach might be exposed to additional personal data which is made available by Client during the provision of Services (and which SafeBreach does not require for the provision of the Services).

4. The categories of data subjects to whom the processed personal data relates to are as follows:
Client employees and internal infrastructure users (such as contractors and vendors with user accounts).
5. The obligations and rights of Client are as set forth in the Terms, herein and in the GDPR.
6. SafeBreach's sub-processors engaged for the purpose of processing personal data: see Appendix C.

Appendix B

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

SafeBreach is ISO 27001 certified and has just completed an audit for SOC 2 Type II at the end of August 2022 (a report is expected by end of October 2022).

We follow best practice information security standards and have a set of policies and procedures that align with the abovementioned standards that we enforce and comply with.

SafeBreach has extensive security measures to protect our AWS cloud production environment that include strict identity-based access control, data encryption in transit and at rest, network protection, logging and monitoring, and more.

We are happy to share our compliance reports and certificate as well as answer any additional questions that arise regarding our compliance posture.

We also invite you to review and subscribe to the SafeBreach Trust Center at https://security.safebreach.com.

Appendix C

List of Sub-Processors

Name	Description of the Subprocessor's activity	Location where Processing will occur (country)
1. AWS	Cloud Hosting Service Provider	USA
2. Salesforce	Customer Support portal	Frankfurt Germany
3. Gainsight	Customer Experience System	USA
4. SafeBreach Ltd.	R&D and maintenance and support services	Israel