Updated February, 25th 2026

SUPPLY-SIDE
DATA PROCESSING ADDENDUM (DPA)

This Data Processing Addendum (the "**DPA**") form with the Term Sheet and related Special Terms, the General Terms and Conditions and related schedules shall form the agreement or contract (the "**Agreement**") between Gadsme SAS and its affiliated companies under the name Gadsme ("**Gadsme**"), and any supply-side partner-either a Supply Partner or a Publisher- undersigned below ("**Supply Side Partner**"). Supply Side Partner and Gadsme may also be referred to herein as a "**Party**"; and collectively as the "**Parties**".

This Data Processing Addendum was updated on February, 25th 2026 and applies to all Supply Partner using Gadsme's Services.

1. The terms and conditions in this DPA, are entered into between Gadsme SAS on behalf of itself and any affiliates that are providing Services (as defined below) to any Supply Side Partner and You ("**Supply Side Partner** ", "**You**"), pursuant to the terms of the Agreement (defined below).
2. This DPA together with the Term Sheet, the Gadsme's Supply-Side (Publisher or Supply Side) General Terms and Conditions, constitute a legally binding agreement between the parties and governs Your use of the Gadsme Services and the parties processing of any personal data under the Agreement. Supply Side Partner agrees that this DPA is like any written negotiated agreement signed by You and agrees to enter into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of any group companies or affiliates that use the Services. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

The Parties agree that this DPA is designed to set forth the Parties` obligations resulting from Applicable Laws.

This DPA will commence on the date of signature of the Principal Agreement or as otherwise agreed between the Parties in writing and will continue until terminated in accordance with the terms of the Principal Agreement (respectively, "**Effective Date**", "**Term**").

1. DEFINITIONS

In this DPA, the following terms shall have the following meanings:

"EEA" means the European Economic Area and Switzerland.

"GDPR" means the General Data Protection Regulation (EU) 679/2016.

"Applicable Data Protection Laws" means all applicable laws governing the handling of Personal Data, including without limitation:

(i) the EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**") and the GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any national laws made under or pursuant to (i) or (ii) (in each case, as superseded, amended or replaced); (iv) the California Consumer Privacy Act of 2018, California Civil Code §1798.100 et seq. ("**CCPA**"), together with any amending or replacement legislation, including the California Privacy Rights Act of 2020 ("**CPRA**") and any regulations promulgated thereunder; (v) other applicable US privacy state laws; (vi) the rules, codes and guidelines of the European Interactive Digital Advertising Alliance ("**EDAA**"); and (vii) the Network Advertising Initiative ("**NAI**").

"Affiliate" means any legal entity directly or indirectly controlling, controlled by or under common control with a Party to the Agreement, where "control" means the ownership of a majority share of the voting stock, equity, or voting interests of such entity.

"Personal Data" shall mean any information that is capable of identifying an individual, including but not limited to, IP addresses, location data, device identifiers, cookie IDs or other identifiers as defined in Applicable Laws.

"Controller" means a person or entity which determines the purposes and the means of processing of Personal Data.

"Processor" means a person or entity which performs the processing of Personal Data on behalf of the Controller.

"Personnel" shall mean any staff (including, without limitations, temporary, casual and unpaid workers) and sub-contractors employed or appointed by the Party.

"Principal Agreement" or **"Agreement"** shall mean the General Terms and Conditions, the Term Sheet, the Special Terms, and related Schedules shall together.

The terms **"Data Subject (s)", "Supervisory Authority", "Processing"** and **"Personal Data Breach"** shall have the meanings ascribed to them on the Applicable Laws. To the extent that the CCPA is applicable, the definition of **"Personal Data"** includes **"Personal Information";** the definition of **"Data Subject"** includes **"Consumer";** the definition of **"Controller"** includes **"Business";** and the definition of **"Processor"** includes **"Service Provider",** all as defined under the CCPA**.**

"Services" mean services provided pursuant to the terms of the Agreement in connection with the use of Gadsme Mobile Advertising Network by the Supply Side Partner.

"Standard Contractual Clauses" or **"SCCs"** means depending on the circumstances applicable to the Supply Side Partner, any of the following:

(a) UK Standard Contractual Clauses, and

(b) 2021 Standard Contractual Clauses, where:

"UK Standard Contractual Clauses" or **"UK SCCs"** means Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision UK IDTA available here or as updated, amended, replaced or superseded from time to time by the competent UK regulatory authority.

"2021 Standard Contractual Clauses" or **"2021 SCCs"** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914 available here or as updated, amended, replaced or superseded from time to time by the European Commission.

"Sub-processor" shall mean a party appointed by a processor or service provider to process personal data on behalf of that processor or service provider.

"Supply Side Partner" means any entity providing advertising inventory to Gadsme, whether:
(i) as owner and operator of digital Properties on which Gadsme technology is implemented ("**Publisher**"), or
(ii) as intermediary (including but not limited to SSPs, resellers or aggregators) providing directly or indirectly access to advertising inventory on behalf of such owner ("**Supply Partner**").

"Security Measures" means the provisions set out in Appendix 2 to this DPA

"User" User pertains to end-users of digital properties from which advertising inventory is made available to Gadsme by the Supply Side Partner that viewed advertising and/or content placed and displayed within the Advertising Inventory supplied by the Supply Side Partner (as defined in the Principal Agreement) via Gadsme's Services (including mobile SDK, as defined in the Principal Agreement) (also referred to as **"Data Subject").**

"User Personal Data" (also used herein as "User('s) Data" for convenience) shall have the meaning of such term or like terms set forth in Data Protection Laws, (including, e.g. "Personal Data" as defined under the GDPR) that is collected by the Supply Side Partner and/or transmitted to Gadsme in connection with the advertising inventory supplied under the Agreement, including through Gadsme's SDK where applicable which include User IP address, User online identifiers such as device ID, advertising identifiers such as AAID/IDFA, and other information pertaining to the User's device and interaction with the application and/or advertising.

2. SCOPE OF THE ADDENDUM

2.1 EU/EEA operations. For operations carried out in the European Union and/or in the European Economic Area (EU/EEA), this Addendum is applicable to the extent that (i) EU Data Protection Law applies to the Processing of User Personal Data, including if (a) the Processing is in the context of the activities of an establishment of either Party in the European Economic Area ("EEA") and/or (b) the Personal Data relates to Data Subjects who are in the EEA and the Processing relates to the offering to them of goods or services or the monitoring of their behavior in the EEA by or on behalf of a Party; or (ii) any other EU Data Protection Law applies to the User Personal Data.

2.2 United States (US) operations. For the purposes of operations carried out in the US, Supply Side Partner is a "Business", Gadsme is a "Third Party", and Users are "Consumers", as defined in CCPA. The references to "Consent Signal" included in Section 6 (Gadsme's Specific Obligations) and all related stipulations shall be construed with regards to opt-out signals, as applicable under CCPA as amended and eligible US Privacy Laws. Operations carried out in the US shall be performed in accordance with the provisions of US State Laws and in accordance with the stipulations set forth in this Addendum, except for Section 3.1 (Joint Data Controllers), Section 5.2 (Consent collection), Section 8 (International Transfers) and Section 9.2 (Data Subject's Privacyc Rights), which are expressly declared non-applicable.

2.3 Rest of the World. The stipulations of this Addendum are applicable to the operations carried out in the remainder of territories where the Services are performed, excluding EU/EEA and US ("Rest of the World"), except for Section 3.1 (Joint Data Controllers), Section 5.2 (Consent collection), Section 8 (International Transfers) and Section 9.2 (Data Subject's Privacy Rights), which are expressly declared non-applicable unless otherwise provided for under Applicable Data Protection Laws.

2.4 Purpose limitation. The Parties shall ensure that they will Process User Personal Data solely for the purposes contemplated in the Principal Agreement, this Addendum or as otherwise agreed to in writing by the Parties.

2.5 For the avoidance of doubt, this Addendum and the obligations hereunder do not apply to aggregated reporting or depersonalized statistics a Party may provide to the other Party in connection with the provision of the Services.

3. ROLES AND RESPONSIBILITIES

3.1 Conditional Joint Controllership

Where Gadsme's SDK or equivalent technology is directly implemented on digital properties operated and controlled by the Supply Side Partner, the Parties shall act as Joint Controllers solely for the operations of reading and/or writing information on the User's device ("Purpose 1 – Store and access information on the device"). This joint responsibility is limited to (i) the setting of the mobile SDK (and/or of any applicable technology provided by Gadsme pursuant to the Principal Agreement), (ii) the obtention of the legal basis and (iii) the management

of Data Subject's privacy rights, in relation to the User's Data processed pursuant to "Purpose 1 – Store and access information on the device" only. In accordance with Applicable Data Protection Laws, the Parties agree to detail their respective obligations and responsibilities within Schedule 2 of this DPA.

Where the Supply Partner acts solely as intermediary and does not implement nor control the implementation of Gadsme technology on digital properties, the Parties shall act as Independent Controllers.

3.2 Independent Data Controllers. For the remainder of the operations carried out in EU/EEA, and for the integrality of the operations carried out in the US and Rest of the World, altogether subject to this Addendum and listed in Schedule 1, the Parties will independently determine the purposes and means of the Processing of User Personal Data, therefore acting as Independent Data Controllers. As such, each Party shall be individually and separately responsible for complying with the obligations that apply to it, in accordance with the Applicable Data Protection Laws.

3.3. Disclaimers. For the sake of clarify, (i) Gadsme is not responsible for operations carried out by Supply Side Partner prior to the initialization of Gadsme's SDK and the associated collection of User Data, since Gadsme does not determine the purposes and means of such operations and (ii) Supply Side Partner is not responsible for operations carried out by Gadsme after the collection of the Users' consent and the withdrawal of the latter and associated collection/processing of User's Data, since it does not determine the purposes and means of such operations.

4. OBLIGATIONS IN RELATION TO THE PROCESSING OF PERSONAL DATA

For the performance of their respective obligations under the Principal Agreement, the Parties shall, at all times, comply with the provisions of Applicable Data Protection Laws, including:

1. Each Party shall maintain a publicly accessible privacy policy on its mobile applications and/or websites, that is available via a prominent link that satisfies transparency disclosure requirements of Applicable Data Protection Law.
2. Each Party is responsible for identifying, documenting, and Processing User Personal Data in accordance with an appropriate lawful basis for the processing of each User's Personal Data and comply with all applicable opt-in and/or opt-out requirements it is subject to pursuant to Applicable Data Protection Laws.
3. Each Party shall ensure the correct application of the principles of minimization and accuracy prior to any Processing of User Personal Data.
4. Each Party shall be fully responsible for any Processors it may use in the performance of the Service. It is the responsibility of each Party to ensure that the Processors provide sufficient guarantees that appropriate technical and organizational measures have been implemented so that the Processing meets the requirements of the applicable regulations. If the Processors do not meet their data protection obligations, the Party concerned remains fully responsible to the User for the performance of their obligations.
5. The Parties shall not (a) place or participate in the placing of targeted advertising (interest-based) to Underage Data Subjects; (b) create or participate in the creation of profiles of Underage Data Subjects; or (c) collect or participate in the collection of personal information from Underage Data Subjects for such purposes. For the purposes of this Agreement, "Underage Data Subject(s)" shall be construed with the meaning conferred on it within Applicable Data Protection Laws, including Data Subjects under 16 as per GDPR and CCPA, and under 18 as per the Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
6. Each Party undertakes to collaborate with the other Party in order to provide the other Party with the necessary elements to carry out any impact assessment relating to data protection.
7. In accordance with the stipulations of Section 7 of this Addendum, each Party undertakes to notify the other Party in the event of Security Incident involving Personal Data Breach.
8. Each Party undertakes to notify the other Party and to cooperate with the other Party in order to respond to any requests for information from or complaint by a Data Protection Authority or any other public authority in any jurisdiction in relation to User's Personal Data.
9. For the purposes of this DPA, the Parties agree that in the performance of the Services under the Agreement, Supply Side Partner and Gadsme may share with each other Personal Data. For the avoidance of the doubts, Supply Side Partner shall not disclose (and shall not permit any data subject to disclose) any special categories of personal data or sensitive data to Gadsme for processing.

v SUPPLY SIDE PARTNER'S SPECIFIC OBLIGATIONS

Notice and Transparency. Supply Side Partner warrants that Users have been provided with transparent notice regarding the collection and processing of Personal Data in accordance with Applicable Data Protection Laws.

Consent collection and transmission. As applicable pursuant to EU Data Protection Laws, Supply Side Partner is responsible for ensuring that legally valid consent has been obtained prior to transmission to Gadsme and to provide Gadsme, upon request, with the evidence of such valid consent being sought. Data Subject's consent shall be obtained, where required under Applicable Data Protection Laws:

(i) directly by the Supply Side Partner where it operates and controls the relevant digital Property, via its Consent Management Platform ("CMP") or equivalent mechanism. Supply Side Partner shall obtain legally valid consent where required, store proof of such consent, and transmit the Consent Signal to Gadsme. Data Subjects may be required to interact with a consent management platform (CMP) in relation to their Personal Data; Gadsme is not responsible for any CMP; or

(ii) by the upstream Publisher or inventory source where the Supply Side Partner acts as intermediary, in which case the Supply Side Partner represents and warrants that it has implemented appropriate contractual and technical measures to ensure that valid consent has been obtained by upstream inventory sources prior to transmission and shall transmit it to Gadsme unaltered, without modification, supplementation, or recreation.

The Supply Side Partner shall not generate, reconstruct, infer or modify any Consent Signal. The Consent Signal shall be transmitted to Gadsme via the IAB TCF string or by any other mutually agreed mechanism ("Consent Signal").

For operations subject to US Privacy Laws, references to Consent Signals shall be construed as applicable opt-out or preference signals.

Evidence and Due Diligence. Supply Side Partner shall, upon reasonable request, provide evidence of the mechanisms implemented to ensure valid consent collection, including documentation of upstream contractual arrangements where applicable.

Regulatory Cooperation. Supply Side Partner shall fully cooperate with Gadsme in the event of any regulatory inquiry, investigation, or complaint relating to consent collection or User Personal Data originating from inventory supplied by the Supply Side Partner, including providing necessary documentation and facilitating communication with upstream publishers where applicable.

Right to Suspend. Gadsme may suspend the processing of Personal Data received from the Supply Side Partner where it has reasonable grounds to believe that consent or transparency requirements are not met.

Upstream Compliance Responsibility. Supply Side Partner acknowledges that it remains solely responsible for ensuring compliance of any upstream publisher or inventory source with Applicable Data Protection Laws.

v GADSME's SPECIFIC OBLIGATIONS

Gadsme will process User Personal Data in accordance with the purposes contemplated in the Principal Agreement and documented in Schedule 1 of this Addendum.

Within the framework of the operations of reading and/or writing information on the User's device, Gadsme undertakes to only access to and/or collect and further process User Personal Data, including advertising identifiers (such as IDFA within the iOS environment, AAID/GAIS within the Android environment, or equivalent advertising identifiers relevant to the technical environment of operation) upon Data Subject's positive consent (to the extent required as per EU Data Protection Laws), obtained by Supply Side Partner and transmitted to Gadsme; or if a lawful legal basis has been established (to the extent required by Applicable Data Protection Laws in the US and Rest of the World).

Gadsme hereby acknowledges that unless a positive Consent Signal has been transmitted by Supply Side Partner upon Data Subject's choice/action originating from Publisher's CMP (as required under EU Data Protection Laws), or unless a lawful legal basis has otherwise been established (to the extent required by Applicable Data Protection Laws in the US and Rest of the World), Gadsme shall not collect and further process Personal Data and online identifiers based on the sole fact that they are made available by the Data Subject's operating system, or on the sole fact that they are technically available and/or readable. This provision specifically pertains to, but is not limited to, advertising and/or device identifiers, such as IDFA within the iOS environment, and AAID/GAIS within the Android environment, made available and/or technically readable by operating systems in relation to tracking permissions. Gadsme shall comply with applicable platform requirements in addition to Consent Signals. Supply Side Partner shall ensure that the implementation of Gadsme technology complies with applicable platform requirements

To the extent required by EU Data Protection Law and US Privacy Laws, Gadsme is responsible for complying with the Consent Signals. Gadsme must respect Consent Signals on an individual basis in real-time and must not rely on a stored version of a previously received Consent Signal to store and/or access information on a device, or to process personal data for any purpose, where a more recent signal has been received from Supply Side Partner. Shall Gadsme be unable to read or process the contents of a received consent signal, Gadsme shall assume that it does not have permission to store and/or access information on a device, or to process personal data for any purpose. Additionally, Gadsme shall refrain from proceeding to such operations if it is unable to act in accordance with the contents of a received Consent Signal.

Gadsme is responsible for the transmission of such Consent Signal to partners/vendors which are part of Gadsme's Buying Partner's network, and which may be solicited and/or activated as part of the Services and operations covered by the Agreement. Such transmission shall be carried out prior to transferring or otherwise making accessible User's Personal Data to such partners/vendors, or simultaneously, and in an unaltered manner (i.e. out without extension, modification, or supplementation of the received consent signal).

To the extent possible as per the state of art and industry practices, Gadsme shall implement contractual and/or technical measures to restrict the sharing of and/or provision of access to and/or retention and further processing capabilities of User's Personal Data to

partners/vendors which have not purchased Supply Side Partner's Ad Inventory, and/or which do not rely on a lawful legal basis to process User's Personal Data.

3. CONFIDENTIALITY

Each Party undertakes to protect the confidentiality of the Personal Data by:

- Taking reasonable steps to ensure that access of its Personnel to the Personal Data is limited to a need to know and/or access basis.
- In particular, the Parties shall ensure that each of the Parties' employees, contractors, (or any other Personnel contracted by the Party's to perform each Party's respective obligations under the Agreement) and receiving such access, are subject to written confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access to and use of Personal Data.

4. DATA SECURITY

Technical and organizational measures. Each Party undertakes to protect the Personal Data received from the other Party under the Agreement and to put in place and maintain appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing or accidental destruction, loss or damage, taking into account the state of the art, the cost of implementation and the nature, scope, context and Purposes of Processing, as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons. Measures to be taken include, in particular, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents.

The security measures implemented by Supply Side Partner are included in Schedule 3 of the Addendum.

Personal Data Breaches. Each Party undertakes to notify the other Party of any incident that involves or is reasonably believed to involve the unauthorized access, use, disclosure, modification, or storage of User's Personal Data that was in its possession or under its control during the Term ("**Personal Data Breach**"). Such notification shall be accompanied by all relevant documentation to enable the Party concerned, if necessary, to notify the competent supervisory authority of the violation and/or to notify Users of the violation. The concerned Party will take measures as may be necessary to mitigate or remedy the effects of the Personal Data Breach. When necessary, the Party shall closely co-operate with the other Party to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

5. DATA RETENTION

In general, Gadsme retain the Personal Data collected for as long as it remains necessary for the purposes set forth above, all under the applicable regulation, or until Supply Side Partner expresses its preference to opt out, where applicable. The retention periods are determined according to the following criteria: (i) For as long as it remains necessary in order to achieve the purpose for which the Personal Data was initially processed. (ii) To comply with our regulatory obligations. (iii) To resolve a claim we might have or a dispute with Supply Side Partner, including any legal proceeding, until such dispute will be resolved, and following, if we find it necessary, in accordance with applicable statutory limitation periods. Please note that except as required by applicable law, we will not be obligated to retain any data for any particular period, and we may delete it for any reason and at any time, without providing you with prior notice if our intention to do so.
Retention periods vary depending on the category of data and applicable legal, contractual or operational requirements. In case of inconsistency, the most specific retention period applicable to a given category of data shall prevail.

6. INTERNATIONAL DATA TRANSFER

Our data servers in which Gadsme host and store the information can be located wherever in the world. The Gadsme's HQ are based in Paris, France in which we may access the information stored on such servers or other systems such as the Gadsme's ERP, CRM, and other systems. In the event that Gadsme needs to transfer Supply Side Partner's Personal Data out of its jurisdiction, Gadsme will take appropriate measures to ensure that Personal Data receives an adequate level of protection as required under applicable law. Furthermore, when Personal Data that is collected within the European Economic Area ("**EEA**") is transferred outside of the EEA to a country that has not received an adequacy decision from the European Commission, Gadsme will take necessary steps in order to ensure that sufficient safeguards are provided during the transferring of such Personal Data, in accordance with the provision of the standard contractual clauses approved by the European Union. Thus, Gadsme will obtain contractual commitments or assurances from the data importer to protect your Personal Data, using contractual protections that EEA and UK regulators have pre-approved to ensure your data is protected (known as standard contract clauses), or rely on adequacy decisions issued by the European Commission.

The Parties agree to ensure that transfers of User's Personal Data outside of the EU or the European Economic Area, Switzerland, or the UK, are made only in accordance with the following:

i. The transfer is to a jurisdiction deemed to have an adequate level of protection as per the European Commission's adequacy decisions (where applicable); or

ii. The transfer is made in accordance with:

a. the EU Standard Contractual Clauses ("EU SCCs"), accessible following this URL https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en); and/or

b. the UK Standard Contractual Clauses (as applicable); and/or

c. the Swiss SCCs (as applicable), and/or

d. an alternate lawful cross-border transfer mechanism in accordance with all applicable laws;

For the purpose of the Standard Contractual Clauses, Supply Side Partner is the "**data exporter**" and Gadsme is the "**data importer**".

in each case, as applicable while taking into consideration the nature and roles of the data exporter and data importer. EU SCCs, UK SCCs and Swiss SCCs are documented in Schedule 4 of this Addendum.

8. TRANSPARENCY AND RIGHTS OF THE DATA SUBJECT

Each Party shall be individually responsible for responding to lawful data protection requests that it receives from the Data Subjects in respect of Personal Data it processes. To the extent that either Party (the "Receiving Party") receives a request relating to processing performed by the other Party, the other party shall provide such information and assistance as it is reasonably necessary to the Receiving Party to enable the Receiving Party to respond to such request in accordance with the Applicable Laws.

If one of the Parties receives requests from a Data Subject to exercise the rights granted under Applicable Data Protection Laws (including right of access, right of rectification, right to withdraw consent, right to opt-out from selling and/or sharing of personal data, right of deletion and right of limitation), it must forward the request to the responsible Party within a period of up to five (5) business days, using the email address indicated in Section 12 – Notification.

If the Data Subject's request pertains the operations falling within the scope of the Parties' Joint Data Controller operations (Purpose 1), and notwithstanding anything to the contrary in this Addendum, the Parties are jointly responsible for the management of Data Subject's request.

9. LIABILITY

9.1 **Compliance Notice and Remediation**
If a Party reasonably believes that the other Party is not complying with its obligations under this DPA, it may notify the other Party in writing and request that the non-complying Party remedy such non-compliance without undue delay. If the non-complying Party fails to provide a satisfactory remediation plan or to implement corrective measures within thirty (30) business days following receipt of such notice, the notifying Party may suspend or terminate all or part of the Principal Agreement in accordance with its terms.

9.2 **General Liability**
Each Party shall be liable to the other Party for damages it causes by any breach of this DPA.

Subject to Section 13 (Limitation of Liability) of the Principal Agreement, each Party agrees to defend and hold harmless the other Party against any and all third-party claims (including claims brought by Supervisory Authorities or Data Subjects) arising out of or relating to that Party's breach of this DPA or Applicable Data Protection Laws.

The breaching Party shall indemnify the other Party for all settlements, judicial awards, damages, liabilities, administrative fines, penalties, costs and expenses (including reasonable legal fees) arising from such breach.

Punitive damages are excluded unless mandatorily imposed by law.

9.3 **Limitation of Liability – General Rule**
Except as expressly set forth in Section 9.4 below, each Party's aggregate liability arising out of or in connection with this DPA shall be subject to the limitation of liability set forth in the Principal Agreement, and in no event shall exceed the amount paid or payable under the Principal Agreement by the Supply Side Partner during the twelve (12) months preceding the event giving rise to the claim.

For the avoidance of doubt, such cap constitutes the total aggregate liability under both the Principal Agreement and this DPA combined.

9.4 **Exclusions from Limitation**
The limitation of liability set forth in Section 9.3 shall not apply to: (i) any breach of Applicable Data Protection Laws resulting from a Party's failure to obtain, ensure, or respect a valid legal basis (including valid consent where required) for the Processing of User Personal Data; (ii) any breach of the Standard Contractual Clauses or any other applicable lawful international data transfer mechanism; (iii) any administrative fines, penalties, corrective measures, or damages imposed by a Supervisory Authority or competent court to the extent arising directly from the breaching Party's violation of this DPA or Applicable Data Protection Laws; (iv) any indemnification obligations relating to third-party claims arising from the breaches described in items (i) through (iii); (v) any gross negligence, wilful misconduct, or fraudulent misrepresentation.

For clarity, each Party shall remain fully and independently liable for its own Processing activities to the extent such Processing does not comply with Applicable Data Protection Laws.

9.5 **Joint Controllership**
Where the Parties act as Joint Controllers pursuant to Section 3.1, each Party shall be liable only for the damage caused by its own processing activities and its own failure to comply with obligations allocated to it under Schedule 2 of this DPA.

Nothing in this DPA shall be interpreted as creating joint and several liability beyond what is required under Applicable Data Protection Laws.

10. SUPERVISORY AUTHORITIES

If the Supply Side Partner receives a complaint, notice or communication from a competent data protection authority which relates to the processing of Personal Data in the context of Gadsme Services under the agreement, it shall, to the extent permitted by law, promptly notify Gadsme and provide such information as may reasonably requested.

Both Parties agree to reasonably cooperate and assist each other in relation to any regulatory inquiry, complaint or investigation concerning the Personal Data shared between the Parties.

11. TERMINATION

The term of this Addendum will take effect on the date of execution of the Principal Agreement and will remain in effect until the Principal Agreement is terminated., provided however, that each Party's obligations under this DPA will apply for so long as the other Party has access to its Personal Data.

Upon termination or expiry of this Addendum, each Party may continue to process User Personal Data provided that such Processing complies with the requirements of this Addendum (Retention Period determined within Schedule 1) and applicable Data Protection Law.

12. NOTIFICATION

Any notification relating to the performance of the Parties' respective and/or mutual obligations under this Addendum should be performed using the following addresses:

- Notification to Supply Side Partner:
- Notification to Gadsme: dpo@gadsme.com

13. ORDER OF PRECEDENCE

1. Nothing in this DPA reduces each Party's obligations under the Agreement in relation to the protection of Personal Data.

2. Subject to Section 9, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

3. Each Party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to any limitation of liability as set forth in the Agreement and any reference to such limitation of liability of a Party means the aggregate liability of the Party under the Agreement and this DPA together. Additionally, each Party shall be independently liable for its own Processing of Personal Data to the extent such Processing does not comply with Applicable Laws.

14. 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.

15. LAW AND JURISDICTION

This DPA (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the same laws applicable to the Agreement. Any dispute, controversy, proceedings or claim between the Parties relating to this DPA (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of the jurisdiction set forth in the Agreement.

16. MISCELLANEOUS

This Addendum and the Agreement shall constitute the entire agreement between the Parties with respect to the subject matter hereof, and this Addendum and the Principal Agreement supersede all prior agreements or representations, oral or written, regarding such subject matter.

The Parties shall agree that electronic format shall be deemed an acceptable means of communication in the execution or sending of an addition or modification to the terms of this Addendum.

Any change to this Addendum can only be agreed upon by the Parties in writing.

The Parties' authorized representatives are deemed to have executed this Addendum as of the Effective Date.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the later date set out below.

Gadsme:	**Supply Side Partner (Publisher or Supply Partner) :**
Name:	**Name:**
Signature:	**Signature:**
Date:	**Date:**

Schedule 1

Details of Processing

1. **Nature and Purpose of the Processing. Frequency of the transfer.** Gadsme will Process Supply Side Partner `s Personal Data as necessary to provide the Service under the Agreement. The Personal Data can be transferred on a continuous basis as necessary for the performance of Service, commercial and or legal matters.

2. **Processing Activities.** Supply Side Partner`s Personal Data will be subject to the basic processing activities necessary for the provision of Gadsme Services, including, without limitation, enabling Demand Partners, DSPs and other authorised advertising partners, and other supply partners to market, sell and buy advertising inventory, provision of advertising or marketing services, auditing related to interactions with the Supply Side Partner, legal compliance, detecting and protecting against security incidents, fraud, and illegal activity, performing services such as account servicing, processing orders and payments, and analytics, internal research for technological improvement, internal operations, activities to maintain and improve our services and other certain one-time uses.

3. **Duration of Processing.** Data is processed and retained for 5 years in order to provide the services, administrative, commercial and legal purposes.

4. **Categories of Data Subjects.** Supply Side Partner's end users and/or End users of digital properties from which advertising inventory is supplied under the Agreement.
   The Services has different automated retention/deletion periods for different types of data and settings but in no event is personal data retained longer than is necessary.

5. **Retention Period.** Supply Side Partner: The aforementioned Data is processed and retained for 365 days. The logs tracking the events are stored 365 days for fraud prevention purposes. Gadsme: The aforementioned Data is processed and retained for 5 years for raw bid data, 2 years for the logs, and 5 years for contractual and fraud data for administrative, commercial and legal purposes.

6. **Categories of Personal Data.** Supply Side Partner`s data which can be provided to Gadsme for provision of Services, including the following attributes of the Bid Request, which can be considered as personal data: device identifiers such as mobile advertising IDs, IP address, IDFA, Google Advertising ID, UDID and other unique identifiers, user agent, detailed geo location, language information, network, device mark and model, device connection, OS type and version, time and date of access and ad view, information about the other apps that a user have or currently has installed on its device, when possible and allowed by End User: year of birth, gender; city and zip data, context of the ads, category and genre of a game, analytics data (session start, session end, clicks etc…), information about the ads a user have already been displayed, General and non-personal activity log Information unique to Users that is automatically collected.

7. **Sensitive Data or Special Categories of Data.** Supply Side Partners are prohibited from including sensitive data or special categories of data in the data transferred to Gadsme.

8. **Sub-processors.** The Supply Side Partner`s Personal Data can be also transferred to sub-processors.

9. **Nature of Processing operations :** Collection, storage, organization, analysis, modification, retrieval, disclosure, communication, and other uses in performance of the Services as set out in the Principal Agreement

10. **Purposes of User Personal Data Processing :** The terminology and numbering follow the order of the purposes listed by IAB Transparency and Consent framework V2 in the EU, which are used by Supply Side Partner as a Publisher, and are which may be used by Gadsme for the purposes of providing the Service:

Purpose 1 - Store and access information on the device (Consent based)

Purpose 2 - Use limited data to select advertising (contextual advertising operations) (Consent based if involving ID-based frequency capping, Legitimate Interest if performed without ID-based frequency capping)

Purpose 3 - Create profiles for personalized advertising (Consent based)

Purpose 4 - Use profiles to select personalized advertising (Consent based)

Purpose 7 - Measure advertising performance (Consent based)

Purpose 9 - Understand audiences through statistics or combinations of data from different sources (Consent based)

Purpose 10 - Develop and improve products (advertising platform) (Consent based)

Special Purpose 1 - Ensure security, prevent and detect fraud, and fix errors (Legitimate Interest)

Special Purpose 2 - Deliver and present advertising and content (Legitimate Interest)

Special Purpose 3 – Save and communicate privacy choices

Special Feature 1 (as applicable) - Use precise geolocation data (based on consent obtained by Publisher)
Special Feature 2 - Actively scan device characteristics for identification (based on consent obtained by Publisher)
Special Feature 3 - Identify devices based on information transmitted automatically (based on legitimate interest)

Schedule 2 (only applicable when Supply Side Partner is a Publisher)

Joint Data Controllership for Purpose 1 - Store and access information on the device

Operation	**Responsibility**	
	Supply Side Partner acting as a Publisher	**Gadsme**
Provision of SDK		X
Implementation of SDK	X	X
Parameters/Settings for initialization of SDK	X	
Determination of purposes for setting SDK	X	X
Determination of legal basis for SDK setting	X	X
Provision of information to Data Subjects pertaining to setting of SDK	X	
Collection of Data Subject's consent for setting and operation of SDK (in line with applicable Data Protection Laws and industry standards)	x	
Transmission of Consent Signals and storage of proof of consent	x	
Acknowledgment and further processing of Consent Signals in relation to this Purpose 1.		X
Data Subject exercise of privacy rights (rectification, objection, access, withdrawal consent) in relation to this Purpose 1.	x Note: Supply Side Partner is designated herein as main point of contact for those Data Subjects rights and will pass on the information to Gadsme promptly	x
Liability (damage caused to Data Subjects by the processing and supervisory authorities' fines, restricted to the operations and responsibilities carried out as Joint Data Controllers, as per the roles and responsibilities delineation set forth in this Schedule 2)	x Limited solely to operations carried out by Supply Side Partner as per this Schedule 2.	x Limited solely to operations carried out by Gadsme as per this Schedule 2.

For avoidance of doubt, joint responsibility for the operations falling within the scope of Purpose 1 (Store and/or access information on a device, as described in the above matrix) is imposed on such processing operations since the Parties jointly define the purposes and/or means of such processing operations, furtherly allowing Gadsme and Publisher to respectively carry out the following operations, as Independent Controllers (as provided for in Section 3.2 of the DPA):

(i) Gadsme to process and/or send the End-User data to Demand partners according to consents provided by End-users to Publisher in order to sell the Publisher's Ad Inventory and authorize the Demand partners to, for the following purposes:

- Purpose 2 - Use limited data to select advertising (based on consent or legitimate interest obtained by Publisher)

- Purpose 3 - Create profiles for personalized advertising (based on consent obtained by Publisher)

- Purpose 4 - Use profiles to select personalized advertising (based on consent obtained by Publisher)

- Purpose 7 - Measure Ad performance; (based on consent obtained by Publisher)

- Purpose 9 - Understand audiences through statistics or combinations of data from different sources including allowing cross-device targeting(Consent based)

- Purpose 10 - Develop and improve services (based on legitimate interest)

- Special Purpose 1 - Ensure security, prevent and detect fraud and fix errors (based on legitimate interest)

- Special Purpose 3 – Save and communicate privacy choices

- Special Feature 1 (as applicable) - Use precise geolocation data (based on consent obtained by Publisher)

- Special Feature 2 - Actively scan device characteristics for identification (based on consent obtained by Publisher)

- Special Feature 3 - Identify devices based on information transmitted automatically (based on legitimate interest)

(iii) Publisher to:

- Implement a Consent Management Platform permitting to collect End-User consent to the above-mentioned processing and to pass opt out or refusals.

- Collect and send to Gadsme data collected from End-Users based on their consent or legitimate interest (depending on the eligible legal basis for that purpose) and in relation to the above-listed purposes

Schedule 3

Technical & Organisational Security Measures

Where applicable, this Schedule 3 will serve as Annex II to the Standard Contractual Clauses. The following table provides more information regarding Gadsme`s technical and organisational security measures set forth below. In all cases, the data importer uses various security technologies and procedures that help protect personal data from unauthorised access, use, disclosure, alteration or destruction.
For example:

1. Physical Access Controls. Access to Gadsme's data centers:	- classification of persons who are granted physical access; - electronic access control; - implementation of measures for on-premise security; - alarm device or security service outside service times; - issuance of access ID badges or visitor badges.
2. Logical Access Controls:	- classification and accountability of persons who may access data processing equipment; - approved users are issued with unique credentials, which must not be shared with or communicated to any other person; - regular review to ensure that only those persons who require access to systems are provided with such access; - password protection for devices and system access; - implementation of Gadsme's policies for external contractors; - Gadsme`s agreements with any sub-processors contain strict confidentiality obligations.
3. Data Access Control:	- allocation of separate ID-parameters exclusively to specific functions; - implementation of partial access rights for respective data and functions; - implementation of policy on access- and user-roles; - evaluation of protocols in case of damaging incidents; - access to the data is promptly removed upon termination of relations or change of role; - Gadsme monitors access to applications, tools, and Gadsme resources that process or store customer data.

4. Computer and Network Security:	- controls to manage the use of removable media in order to prevent unauthorised disclosure, modification, removal or destruction of personal data stored on it; - password security procedures; - description of a process to detect any unauthorised access or anomalous use; - effective anti-malware defences to protect computers from malware infection; - monitoring user and system activity to identify and help prevent data breaches; - boundary firewalls to protect computers from external attack and exploitation.
5. Trusted Vendors	Gadsme rely only on vendors who ensure an appropriate level of security of your Data. In this context, we use only secure cloud servers, including AWS cloud – a secure, private cloud platform. Amazon Web Services ("AWS"), OVH cloud and Google Cloud Platform are Gadsme's sub-processors. AWS, OvhCloud and Google Cloud Platform each use various security technologies and procedures to protect personal data and is compliant with third-party assurance frameworks such as ISO 27017 for cloud security, ISO 27018 for cloud privacy, PCI DSS Level 1, and SOC 1, SOC 2, and SOC 3. For more details please see security and privacy policy at www.aws.amazon.com, www.ovhcloud.com, Google Cloud Platform at www.cloud.google.com and Cloudflare at www.cloudflare.com
6. Organisational measures	- Gadsme regularly performs assessments on the effectiveness of administrative, organisational, technical and physical safeguards reasonably designed to protect the services and confidentiality, integrity and availability of personal data. - Gadsme has adopted measures for ensuring accountability, such as implementing data protection policies across the business, maintaining documentation of processing activities, recording and reporting security incidents involving personal data, and appointing a Data Protection Officer.
7. Data Encryption	• Approved Encryption Standards – A documented information security policy is in place that specifies the approved encryption standards and key management practices. • Algorithms like AES, Secure version of TLS, HTTPS, RSA, DSA are used by Gadsme for data encryption. • Data at Rest Encryption – Data at rest on servers is encrypted on demand as per the project or regulation security requirements. • Data in Transit Encryption –Secure version TLS encryption is used to protect information in transit. Secure File Transfer service is used for the transfer of documents. Algorithms like secure version of TLS, HTTPS, PGP, S-MIME are acceptable for encrypting information in transit.

8. Event Log Management	• Event Logging – Logging system events related to privileged access like addition, removal, modification or denial are implemented based on perceived risks and when technically feasible. Critical security events of business-critical systems are logged and reviewed on an incident basis
9. Vulnerability Management	• Vulnerability Assessment Program– Vulnerability management procedure is in place that defines method of identifying, reporting and managing vulnerabilities affecting Gadsme network. Network perimeter scans are performed on a regular basis. The Information Security Team offers security testing services to project teams to assess the security of web applications or hosted environments. Testing is performed to identify common vulnerabilities such as the OWASP Top 10, known service vulnerabilities, logic flaws, and insecure configurations.

Supplementary Measures:

1. If Gadsme receives an order or request to disclose Personal Data transferred under the Agreement ("Transferred Personal Data") to a law enforcement, regulatory, judicial or governmental authority (an "Authority"), whether on a binding or voluntary basis, Gadsme shall:

(a) promptly notify the Supply Side Partner of such Authority's data access request;

(b) inform the Authority that any and all requests or demands for relating to the Transferred Personal Data should be notified to or served upon the Supply Side Partner (as the originating Controller) in writing; and

(c) not provide the Authority with access to Transferred Personal Data unless and until authorised by the Supply Side Partner, save to the extent any such order or request or other legally binding obligation on Gadsme requires Gadsme to do otherwise.

2. In the event Gadsme is under a legal prohibition or a legal compulsion that prevents it from complying with paragraphs 1(a) to 1(a) in full, Gadsme shall use reasonable and lawful efforts to challenge such prohibition or compulsion (and the Supply Side Partner acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request and the reasonable prospects and costs of successfully challenging the prohibition or compulsion).

3. Paragraphs 1 and 2 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Transferred Personal Data, Gadsme has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Gadsme shall notify the Supply Side Partner as soon as practicable following such Authority's access and provide the Supply Side Partner with full details of the same, unless and to the extent Gadsme is legally prohibited from doing so.

4. Gadsme shall not knowingly disclose the Transferred Personal Data in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

5. Gadsme shall have in place, maintain and comply with a policy governing personal data access requests from Authorities which at minimum prohibits:

(a) massive, disproportionate or indiscriminate disclosure of personal data relating to data subjects in the European Economic Area or the United Kingdom; and

(b) disclosure of personal data relating to data subjects in the European Economic Area or the United Kingdom to an Authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such personal data.

6. Gadsme shall have in place and maintain in accordance with good industry practice measures to protect the Transferred Personal Data from unauthorised interception (including in transit from the Supply Side Partner to Gadsme and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept Transferred Personal Data and encryption of Transferred Personal Data whilst in transit to deny attackers the ability to read Transferred Personal Data.

Schedule 4
Standard Contractual Clauses

1. EU SCCS

For the purposes of the EU SCCs, the Parties hereby agree to adopt and incorporate the SCCs to the Agreement, which will be deemed completed with the following information and executed by the Parties as of the Effective Date of this Addendum:

(a) Module One will apply to the extent that the Parties act as Joint and Independent Data Controllers as per the Agreement ;
(b) Supply Side Partner will be referred to as the "Data Exporter" and Gadsme will be referred to as the "Data Importer" in such clauses, with relevant Gadsme name and address details from the Agreement;
(c) in Clause 7, the optional docking clause applies;
(d) in Clause 11, the optional language does not apply;
(e) in Clause 13 referring to Annex 1.C the competent supervisory authority for the EU is the Commission Nationale de l'Informatique et des Libertés "CNIL" (France) unless determined otherwise;
(f) in Clause 16, the EU SCCs are governed by the laws of France;
(g) in Clause 17, disputes will be resolved before the courts of France
(h) Annex I (List of Parties and Description of Transfer) shall be deemed completed with the information set out in Schedule 1 hereafter.
(i) Annex II (Technical and organizational measures) shall be deemed completed with the information set out in Schedule 3 hereafter.
(j) Annex III (List of Sub processors) shall not apply.
(k) to the extent that there is any conflict between this Addendum and/or the Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail;
(l) in Clause 18(b), disputes will be resolved before the courts of Paris, France;

2. UK and Swiss SCCs

Where the UK GDPR applies, SCCs refer to the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) where the UK GDPR means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, therein (the "UK SCCs"). For the sake of clarity, the UK saved GDPR into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019.

Where Swiss DPA applies, SCCs refer to the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs"). For the sake of clarity, Swiss DPA means the Swiss Federal Data Protection Act and its implementing regulations.

In relation to transfers of personal data protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under Section 1 of this Schedule 4 will apply with the following modifications:

(i) References to "Regulation (EU) 2016/679" shall be interpreted as references to UK GDPR and Data Protection Act 2018 ("UK Privacy Laws") or the Swiss DPA (as applicable);
(ii) References to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Privacy Laws or the Swiss DPA (as applicable);
(iii) References to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);
(iv) The term "member state" (whether or not capitalized) shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);
(v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
(vi) References to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);
(vii) In Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and
(viii) With respect to transfers to which UK Privacy Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding 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", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.
(ix) To the extent that and for so long as the EU SCCs as implemented in accordance with Section 1 above cannot be used to lawfully transfer Exporter Data in accordance with the UK GDPR to the Importer, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Schedules 1, 2 and 3 of this DPA.
(x) In relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows in regards with the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum") : (a) apply as completed in accordance with the Principal Agreement; (b) Part 1 is incorporated by reference as follows: tables 1 to 3 shall be completed respectively with the information set out in Schedules 1, 2 and 3 of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party" and (c) is deemed amended as specified by Part 2, which shall be deemed incorporated into and form an integral part of this DPA.
(xi) The illustrative indemnification clause will not apply;
(xii) In Appendix 1 the information shall be as described in subsection 7.3. (b) (vi) below;
(xiii) Schedule 1 (Details of Processing) of this DPA serves as Appendix 1 of the UK SCCs;

(xiv) Schedule 3 (Technical and Organisational Security Measures) of this DPA serves as Appendix 2 of the UK SCCs;
(xv) Table 1 shall be deemed completed with Parties's details from the Agreement;
(xvi) In Table 4, the Parties choose the option "neither Party".

2021 SCCs. For the international data transfers, where the GDPR is applicable and the Personal Data is transferred by the Supply Side Partner to Gadsme via the Service, 2021 SCCs will apply in the following manner:

4. The parties acknowledge that clause 2 of the 2021 SCCs (or clause 10 of the UK SCCs respectively) permits them to include additional business-related terms provided they do not contradict with the SCCs. Accordingly, this section 7.4. sets out the Parties' interpretation of their respective obligations under specific clauses identified below. Where a Party complies with the interpretations set out in this section, that Party shall be deemed by the other Party to have complied with its commitments under the SCCs. Liability. Any claims brought under the SCCs shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event, shall any Party limit its liability with respect to any data subject rights under the SCCs.