



DATA PROCESSING ADDENDUM

This Data Processing Addendum (the “**DPA**”) form with the General Terms and Conditions, the Special Terms and the Purchase Order and related schedules shall form the agreement or contract (the “**Agreement**”) between Gadsme SAS and its affiliated companies under the name Gadsme (“**Gadsme**”), and the partner undersigned below (“**Partner**”). Partner and Gadsme may also be referred to herein as a “**Party**”; and collectively as the “**Parties**”.

This Data Processing Addendum was updated on May, 11th 2023 and applies to all Partners 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 Partners and You (“**Partner**”), pursuant to the terms of the Agreement (defined below).
2. This DPA together with the Agreement, 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. Partner agrees that this DPA is like any written negotiated agreement signed by Partner 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.

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- (iii) any national laws made under or pursuant to (i) or (ii) (in each case, as superseded, amended or replaced);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.

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 by Partner of Gadsme Mobile Advertising Network.

“Standard Contractual Clauses” or “SCCs” means depending on the circumstances unique to the 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 2004/915/EC 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.

“Security Measures” means the provisions set out in Appendix 2 to this DPA.

2. OBLIGATIONS IN RELATION TO THE PROCESSING OF PERSONAL DATA

1. For the purposes of this DPA, the Parties agree that in the performance of the Services under the Agreement, Partner and Gadsme may share with each other Personal Data. For the avoidance of the doubts, no sensitive data or special categories of data shall be transferred by the Partner to Gadsme. 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.
2. The Parties further agree that Partner and Gadsme are each separate and independent Controllers of the Personal Data that both Parties may exchange in the performance of the Agreement and hence responsible for complying with Applicable Laws. For avoidance of doubt, the Parties shall not determine the purposes and the means of Processing together and shall not function in the capacity of Joint Controllers (as defined in the GDPR).
3. Partner represents that the Personal Data which shall be provided by Partner in the performance of the Agreement was collected and processed lawfully including but not limited to by obtaining all necessary consents from Data Subjects and provision of appropriate notices to the Data Subjects in compliance with Applicable Laws and subject to any technical limitations and other exclusions available under Applicable Laws. In particular, the Partner represents and warrants that either: a) to the extent the Personal Data of the EEA Data Subjects is transferred, it is a participant in the IAB Europe Transparency & Consent Framework (“TCF”) and will adhere to TCF rules and guidelines, or b) that it has otherwise obtained any legally required consent to the collection, use and disclosure of the Personal Data to allow Gadsme to process it in connection with the Services. The Partner shall notify Gadsme of any changes in, or revocation of the permission to use, disclose or otherwise process the Personal Data it provided to Gadsme under the Agreement that would impact the ability of Gadsme to comply with this DPA and Applicable Laws.
4. Each Party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under Applicable Laws. Each party shall maintain a publicly accessible privacy policy on its website that is in compliance with Applicable Laws.
5. The Partner shall comply with all the requirements of the Applicable Laws, including but not limited to CCPA or the US Children Online Privacy Protection Act (“COPPA”). The Partner shall not share with Gadsme any personal information (as defined under CCPA or COPPA respectively) of consumers who either: (i) were not provided with any notifications required under CCPA and/or COPPA, or (ii) were not provided with an option to opt out from a sale under the CCPA and in accordance with its requirements. Any (i) notification regarding a consumer’s election pursuant to any privacy related rights available to the consumer under applicable privacy and data protection legislation that Gadsme is required to comply with, (ii) third-party or consumer requests or complaints regarding the processing of personal information, or (iii) government or consumer requests for access to or information about processing of personal information on Gadsme’s behalf, shall be notified to Gadsme by the Partner promptly and in any event in order to allow Gadsme enough time to meet any obligations under the CCPA and/or COPPA.
6. Relationship of the parties: Partner (as the controller in its own right or as the processor who acts under instruction from third party controller(s)) or another business appoints Gadsme as a processor (or sub-processor, as the case may be) to process the personal data described in the Agreement (the “Data”) for the purposes described in the Agreement (or as otherwise agreed in writing by the parties) (the “Permitted Purpose”). Each party shall comply with the obligations that apply to it under Applicable Data Protection Laws. If Gadsme becomes aware that processing for the Permitted Purpose infringes an Applicable Data Protection Law, it shall promptly inform the Partner.

3. CONFIDENTIALITY

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

1. 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.
2. 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

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.

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 You express Your 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 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.

6. INTERNATIONAL DATA TRANSFER

Our data servers in which Gadsme host and store the information can be located wherever in the world. The Company's HQ are based in Paris, France in which we may access the information stored on such servers or other systems such as the Company's ERP, CRM, and other systems. In the event that Gadsme needs to transfer 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.

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

7. PERSONAL DATA BREACHES

1. Each Party shall notify the other Party without undue delay from the moment of becoming aware of any Personal Data Breach with respect to Personal Data received from the other Party. Such notification shall include the following information, to the extent in the possession and control of the Party suffering the Personal Data Breach and to the extent possible: the types and number of Data Subjects affected, the categories of Personal Data affected, the possible cause of the Personal Data Breach, the possible adverse consequences and the likelihood of their occurrence. If the information is not available at the first instance, it shall be provided in phases.
2. Each Party shall cooperate with the other Party, to the extent reasonably requested in relation to notifications to a Supervisory Authority or to Data Subjects which are required following a Personal Data Breach involving Personal Data Processed pursuant to this DPA or otherwise enabling the other Party to comply with its obligations under Applicable Laws.

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.

9. TRANSFERS OF PERSONAL DATA

1. Where the Party's establishment undertaking the data Processing is located outside the EEA or in any other cases in which Processing is being performed in a location is not one which the European Commission ("EC") considers providing adequate protection of Personal Data, it will ensure that any Processing by the Party is governed by:

- ❖ the provisions of the Standard Contractual Clauses (as amended and superseded from time to time); or
- ❖ any other safeguards as applicable, mentioned in the relevant Articles of the GDPR.

2. **UK SCCs.** The parties agree that the UK SCCs will apply to the international data transfers, where UK GDPR is applicable and the Personal Data is transferred by the Partner to Gadsme via the Services, either directly or via onward transfer, to any country or recipient outside of the UK that is not recognized by the competent UK regulatory authority or governmental body for the UK as providing an adequate level of protection for personal data. The UK SCCs will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

(a) The illustrative indemnification clause will not apply.

(b) In Appendix 1 the information shall be as described in subsection 7.3. (b) (vi) below.

(c) Schedule 1 (Details of Processing) of this DPA serves as Appendix 1 of the UK SCCs.

(d) Schedule 2 (Technical and Organisational Security Measures) of this DPA serves as Appendix 2 of the UK SCCs.

(e) Table 1 shall be deemed completed with Parties's details from the Agreement.

(f) In Table 4, the Parties choose the option "neither Party"

3. **2021 SCCs.** For the international data transfers, where the GDPR is applicable and the Personal Data is transferred by the Partner to Gadsme via the Service, 2021 SCCs will apply in the following manner:

(a) Module One (Controller to Controller) will apply to the relations of the parties.

(b) For Module One:

(i) Clause 9 of the SSC shall be deemed inapplicable;

(ii) in Clause 7, the option docking clause will not apply;

(iii) in Clause 11, the optional language will not apply;

(iv) in Clause 17 (Option 1), the Standard Contractual Clauses will be governed by the laws of France;

(v) in Clause 18(b), disputes will be resolved before the courts of Paris, France;

(vi) In Annex I, Part A:

Data Exporter: Partner and authorized affiliates of the Partner.

Contact Details: Contact email indicated in the Partner's account.

Data Exporter Role: The Data Exporter's role is outlined in Section 2.2 of this DPA.

Signature & Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: Gadsme SAS

Contact Details: Gadsme Privacy Team - privacycompliance@Gadsme.com

Data Importer Role: The Data Importer's role is outlined in Section 2.2 of this DPA.

Signature & Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) In Annex I, Part B: the information shall be as described in Schedule 1 to this DPA.

(viii) In Annex I, Part C: applicable competent authorities shall be determined in accordance with the provisions of clause 13 of the 2021 SCCs.

(ix) Schedule 2 to this DPA serves as Annex II of the Standard Contractual Clauses.

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.

10. SUPERVISORY AUTHORITIES

1. If the 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 be requested.
2. 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

This DPA shall terminate automatically upon the termination of the Agreement, 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.

12. 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 10.1, 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.

13. 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.

14. 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.

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.

Schedule 1

Details of Processing

1. **Nature and Purpose of the Processing. Frequency of the transfer.** Gadsme will Process 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.
2. **Processing Activities.** Partner`s Personal Data will be subject to the basic processing activities necessary for the provision of Gadsme Services, including, without limitation, enabling publishers and other supply partners as well as DSPs and other demand partners to market, sell and buy advertising inventory, provision of advertising or marketing services, auditing related to interactions with the 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.** As necessary for the provision of Services under the Agreement.
4. **Categories of Data Subjects.** Partner`s end users and/or End users that visit Publisher`s Websites and games. 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. **Categories of Personal Data.** 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, user agent, geo location, lat and lon (in the geo object), i.e. latitude and longitude coordinates, user ID (including buyer ID), cookie ID, year of birth, gender; city and zip data, type of connection, network, context of the ads, category and genre of a game, language preference of the device, analytics data (session start, session end, clicks etc...), end user behaviours, ad category, any information shared by the Partner, bid price, creative (the advert / image, video or audio).
6. **Sensitive Data or Special Categories of Data.** Partners are prohibited from including sensitive data or special categories of data in the data transferred to Gadsme.
7. **Sub-processors.** The Partner`s Personal Data can be also transferred to sub-processors.

Schedule 2

Technical & Organisational Security Measures

Where applicable, this Schedule 2 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:	<ul style="list-style-type: none"> - 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:	<ul style="list-style-type: none"> - 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 company policies for external contractors; - Gadsme`s agreements with any sub-processors contain strict confidentiality obligations.
3. Data Access Control:	<ul style="list-style-type: none"> - allocation of separate terminals/workstations and of 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, including cloud services.

4. Computer and Network Security:	<ul style="list-style-type: none"> - 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	<p>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.</p> <p>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 and Google Cloud Platform at www.cloud.google.com.</p>
6. Organisational measures	<ul style="list-style-type: none"> - 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.

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 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 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 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 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 Partner as soon as practicable following such Authority's access and provide the 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 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.