Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the subscription agreement, Sightengine's Terms of Service available at https://sightengine.com/policies/terms or other written or electronic agreement (the "**Agreement**"), including any written or electronic service orders, purchase orders or other order forms (each a "**Service Order**") entered into between Sightengine and Subscriber, pursuant to which Sightengine provides Services as defined in the Agreement.

The purpose of this DPA is to reflect the parties' agreement with regard to the processing of Subscriber Personal Data. The parties agree to comply with this DPA with respect to any Subscriber Personal Data that the Sightengine Group may process in the course of providing the Services pursuant to the Agreement. This DPA shall not replace or supersede any data processing addendum or agreement executed by the parties prior to the DPA Effective Date without the prior written consent of the parties (electronically submitted consent acceptable).

This DPA will take effect on the DPA Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Subscriber Data by Sightengine as described in this DPA.

If the Subscriber entity entering into or accepting this DPA is neither a party to a Service Order nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Subscriber entity that is a party to the Agreement executes this DPA.

By signing or accepting the Agreement or this DPA, Subscriber enters into this DPA as of the DPA Effective Date on behalf of itself and in the name and on behalf of its Covered Affiliates if and to the extent the Sightengine Group processes personal data for which such Covered Affiliates qualify as the controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Subscriber" shall include Subscriber and its Covered Affiliates.

1. Definitions

1.1. Capitalized terms used but not defined in this DPA shall have the meaning given to them in the Agreement or applicable Data Protection Laws.

"**Affiliates**" of a party is any entity (a) that the party Controls; (b) that the party is Controlled by or (c) with which the party is under common Control, where "**Control**" means direct or indirect control of fifty percent (50%) or more of an entity's voting interests (including by ownership).

"**Sightengine**" is an Image and Video Analysis Service owned and operated by Kozelo SAS, a French société par actions simplifiées incorporated in France ("Sightengine", "we" , or "us"). For the purpose of this Agreement, "Sightengine" refers to Kozelo SAS or any other Kozelo Affiliate that is a party to the Agreement, as applicable.

"**Sightengine Group**" means Sightengine and its Affiliates engaged in the processing of Subscriber Personal Data in connection with the subscribed Services.

"**Covered Affiliate**" means any of Subscriber's Affiliate(s) which (a) is subject to the Data Protection Laws, and (b) is permitted to use the Services pursuant to the Agreement between

Subscriber and Sightengine, but has not signed its own Service Order with Sightengine and is not a "Subscriber" as defined under the Agreement.

“Data Incidents” means a breach of Sightengine’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Subscriber Data transmitted, stored or otherwise processed by Sightengine. “Data Incidents” will not include unsuccessful attempts or activities that do not compromise the security of Subscriber Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Data Protection Laws" means all applicable data protection and privacy laws and regulations, including EU Data Protection Laws.

“**DPA Effective Date**” means, as applicable, (a) May 25, 2018 if Subscriber clicked to accept or the parties otherwise agreed to this DPA prior to or on such date; or (b) the date on which Subscriber clicked to accept or the parties otherwise agreed to this DPA, if such date is after May 25, 2018.

“**EEA**” means the European Economic Area.

“**EU Data Protection Laws**” means laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the processing of Personal Data under the Agreement, including European Directives 95/46/EC and any legislation and/or regulation which amends, replaces or re-enacts it (including the GDPR).

"**GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC effective as of May 25, 2018 and any legislation and/or regulation which amends, replaces or re-enacts it.

“**Security Documentation**” means all documents and information made available by Sightengine to demonstrate compliance by Sightengine with its obligations under this DPA, including the Security Measures, Additional Security Information and any third-party certifications or audit reports, as applicable.

“**Security Measures**” means the administrative, technical and physical safeguards adopted by Sightengine applicable to the Services subscribed by Subscriber as described and made available at https://sightengine.com/faq or as otherwise made available by Sightengine. The Security Measures as of April 25, 2018 is attached to this DPA as Attachment 2.

“**Sub-processor**” means any third-party engaged by Sightengine or a member of the Sightengine Group which processes Subscriber Data in order to provide parts of the Services.

“**Subscriber**” means the subscriber entity party to the Agreement. Subscriber may also be referred to as “**Customer**” in the Agreement from time to time.

“**Subscriber Data**” has the meaning given to it in the Agreement or, if no such meaning is given, means data submitted by or on behalf of Subscriber to the Services under the Subscriber’s Sightengine account for Services. Subscriber Data may also be referred to as “**Customer Data**” in the Agreement from time to time.

“**Subscriber Personal Data**” means the personal data contained within Subscriber Data. Subscriber Personal Data may also be referred to as “**Customer Personal Data**” in the Agreement from time to time.

"**Term**" means the period from the DPA Effective Date until the end of Sightengine's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended, or in trial, or on a free plan, or on a free account and any post-termination period during which Sightengine may continue providing the Services for transitional purposes.

1.2. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this DPA have the meanings given in the GDPR, in each case irrespective of whether other Data Protection Laws apply.

2. Personal Data Processing Terms

2.1. The parties agree that if the EU Data Protection Laws apply to the processing of Subscriber Personal Data, the parties acknowledge and agree that:

2.1.1. Subscriber is the controller and Sightengine and the Sightengine Group are the processor of the Subscriber Personal Data and Sightengine or a member of the Sightengine Group may engage Sub-processors pursuant to Section 7 (Sub-processors).

2.1.2. The subject-matter of the data processing covered by this DPA is the provision of the Services and the processing will be carried out for the duration of the Agreement or so long as Sightengine is providing the Services. Attachment 1 of this DPA sets out the nature and purpose of the processing, the types of Subscriber Personal Data Sightengine processes and the categories of data subjects whose Personal Data is processed.

2.1.3. Each party will comply with the obligations applicable to it under the EU Data Protection Laws, including with respect to the processing of Subscriber Personal Data.

2.1.4. If the GDPR is applicable, Sightengine will process Subscriber Personal Data in accordance with the requirements of the GDPR directly applicable to Sightengine's provision of Services. Notwithstanding anything to the contrary set forth in this DPA, in the event of a conflict or clarification of definitions, the GDPR shall apply only as of May 25, 2018.

2.1.5. If Subscriber is a processor itself, Subscriber warrants to Sightengine that Subscriber's instructions and actions with respect to the Subscriber Personal Data, including its appointment of Sightengine as another processor, have been authorized by the relevant controller.

2.1.6. For the avoidance of doubt, Subscriber's instructions to Sightengine for the processing of Subscriber Personal Data shall comply with all applicable laws, including the EU Data Protection Laws. As between Sightengine and Subscriber, Subscriber shall be responsible for the Subscriber Data and the means by which Subscriber acquired Subscriber Data.

2.1.7. For the purposes of this DPA, the following is deemed an instruction by Subscriber to process Subscriber Personal Data (a) to provide the Services; (b) as further specified via Subscriber's use of the Services (including the Services' user interface dashboard and other functionality of the Services); (c) as documented in the Agreement (including this DPA and any Service Order that requires processing of Subscriber Personal Data); and (d) as further documented in any other written instructions given by Subscriber (which may be specific instructions or instructions of a general nature as set out in this DPA, the Agreement or as otherwise notified by Subscriber to Sightengine from time to time), where such instructions are consistent with the terms of the Agreement.

2.1.8. When Sightengine processes Subscriber Personal Data in the course of providing the Services, Sightengine will:

2.1.8.1. Process the Subscriber Personal Data only in accordance with (a) the Agreement and (b) Subscriber's instructions as described in Section 2.1.7, unless Sightengine is required to process Subscriber Personal Data for any other purpose by European Union or member state law to which Sightengine is subject. Sightengine shall inform Subscriber of this requirement before processing unless prohibited by applicable laws on important grounds of public interest.

2.1.8.2. Notify Subscriber without undue delay if, in Sightengine's opinion, an instruction for the processing of Subscriber Personal Data given by Subscriber infringes applicable EU Data Protection Laws.

2.2. The parties acknowledge and agree that the parties will comply with all applicable laws with respect to the processing of Subscriber Personal Data.

3. Data Security

3.1. Security Measures

3.1.1. Sightengine will implement and maintain appropriate technical and organizational measures designed to protect or secure (i) Subscriber Data, including Subscriber Personal Data, against unauthorized or unlawful processing and against accidental or unlawful loss, destruction or alteration or damage, unauthorized disclosure of, or access to, Subscriber Data, and (ii) the confidentiality and integrity of Subscriber Data, as set forth in the Security Measures. Sightengine may update or modify the Security Measures from time to time provided that such updates and modifications will not materially decrease the overall security of the Services. The most up to date Security Measures will be made available at https://sightengine.com/faq.

3.1.2. In addition to the Security Measures, Sightengine will, from time to time, make additional security guidelines available that provide Subscriber with information about, in Sightengine's opinion, best practices for securing, accessing and using Subscriber Data including best practices for password and credentials protection ("**Additional Security Information**").

3.1.3. Sightengine will take reasonable steps to ensure the reliability and competence of Sightengine personnel engaged in the processing of Subscriber Personal Data.

3.1.4. Sightengine will take appropriate steps to ensure that all Sightengine personnel engaged in the processing of Subscriber Personal Data (i) comply with the Security Measures to the extent applicable to their scope of performance, (ii) are informed of the confidential nature of the Subscriber Personal Data, (iii) have received appropriate training on their responsibilities and (iv) have executed written confidentiality agreements. Sightengine shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.2. Data Incidents

3.2.1. If Sightengine becomes aware of a Data Incident, Sightengine will: (a) notify Subscriber of the Data Incident without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Subscriber Data.

3.2.2. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and, as applicable, steps Sightengine recommends Subscriber to take to address the Data Incident.

3.2.3. Notification(s) of any Data Incident(s) will be delivered to Subscriber in accordance with the "Manner of Giving Notices" Section of the Agreement or, at Sightengine's discretion, by direct communication (for example, by phone call or an in-person meeting). Subscriber is solely responsible for ensuring that any contact information, including notification email address, provided to Sightengine is current and valid.

3.2.4. Sightengine will not assess the contents of Subscriber Data in order to identify information subject to any specific legal requirements. Subscriber is solely responsible for complying with incident notification laws applicable to Subscriber and fulfilling any third-party notification obligations related to any Data Incident(s).

3.2.5. Sightengine's notification of or response to a Data Incident under this Section 3.2 (Data Incidents) will not be construed as an acknowledgement by Sightengine of any fault or liability with respect to the Data Incident.

3.3. Subscriber's Security Responsibilities and Assessment of Sightengine

3.3.1. Subscriber agrees that, without prejudice to Sightengine's obligations under Section 3.1 (Security Measures) and Section 3.2 (Data Incidents):

3.3.1.1. Subscriber is solely responsible for its use of the Services, including: (i) making appropriate use of the Services and any Additional Security Information to ensure a level of security appropriate to the risk in respect of the Subscriber Data; (ii) securing the account authentication credentials, systems and devices Subscriber uses to access the Services; and (iii) backing up the Subscriber Data; and

3.3.1.2. Sightengine has no obligation to protect Subscriber Data that Subscriber elects to store or transfer outside of Sightengine's and its Sub-processors' systems (for example, offline or on- premises storage).

3.3.2. Subscriber is solely responsible for reviewing the Security Measures and evaluating for itself whether the Services, the Security Measures, the Additional Security Information and Sightengine's commitments under this Section 3 (Data Security) will meet Subscriber's needs, including with respect to any security obligations of Subscriber under the Data Protection Laws. Subscriber acknowledges and agrees that the Security Measures implemented and maintained by Sightengine as set out in Section 3.1 (Security Measures) provide a level of security appropriate to the risk in respect of the Subscriber Data.

3.4. Subscriber Assessment and Audit of Sightengine compliance

Upon Subscriber's written request, at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Sightengine will make available to Subscriber that is not a competitor of Sightengine (or Subscriber's independent, third-party auditor that is not a competitor of Sightengine) information regarding the Sightengine Group's compliance with the obligations set forth in this DPA.

3.5. Subscriber's Audit Rights

3.5.1. No more than once per year, Subscriber may contact Sightengine in accordance with the "Manner of Giving Notices" Section of the Agreement to request an audit of the procedures relevant to the protection of Subscriber Data. Subscriber shall reimburse

Sightengine for any time expended for any such audit. Before the commencement of any such audit, Subscriber and Sightengine shall mutually agree upon the scope, timing, and duration of the audit, that reasonably does not interfere with normal business operations, in addition to the reimbursement rate for which Subscriber shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Sightengine. Subscriber shall promptly notify Sightengine with information regarding any non- compliance discovered during the course of an audit.

3.5.2. Subscriber may conduct such audit (a) itself, (b) through an Affiliate that is not a competitor of Sightengine or (c) through an independent, third-party auditor that is not a competitor of Sightengine.

3.5.3. Subscriber may also conduct an audit to verify Sightengine's compliance with its obligations under this DPA by reviewing the Security Documentation.

4. Return or Deletion of Subscriber Data

4.1. Sightengine will enable Subscriber to delete during the Term Subscriber Data in a manner consistent with the functionality of the Services. If Subscriber uses the Services to delete any Subscriber Data during the Term and that Subscriber Data cannot be recovered by Subscriber, this use will constitute an instruction to Sightengine to delete the relevant Subscriber Data from Sightengine's systems in accordance with applicable law. Sightengine will comply with this instruction as soon as reasonably practicable within a maximum of 90 days, unless the European Union or member state law requires storage.

4.2. Upon expiry of the Term or upon Subscriber's written request, subject to the terms of the Agreement, Sightengine shall either (a) return (to the extent such data has not been deleted by Subscriber from the Services) or (b) securely delete Subscriber Data, to the extent allowed by applicable law, in accordance with the timeframes specified in Section 4.3, as applicable.

4.3. Sightengine will, after a recovery period of up to 30 days following expiry of the Term, comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless European Union or member state law requires storage. Without prejudice to Section 5 (Data Subject Rights; Data Export), Subscriber acknowledges and agrees that Subscriber will be responsible for exporting, before the Term expires, any Subscriber Data it wishes to retain afterwards.

5. Data Subject Rights; Data Export

5.1. As of the DPA Effective Date for the duration of the period Sightengine provides the Services:

5.1.1. Sightengine will, in a manner consistent with the functionality of the Services, enable Subscriber to access, rectify and restrict processing of Subscriber Data, including via the deletion functionality provided by Sightengine as described in Section 4 (Return or Deletion of Subscriber Data), and to export Subscriber Data;

5.1.2. Sightengine will, without undue delay, notify Subscriber, to the extent legally permitted, if Sightengine receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure, data portability, objection to the processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"); and

5.1.3. if Sightengine receives any request from a data subject in relation to Subscriber Personal Data, Sightengine will advise the data subject to submit his or her request to Subscriber and Subscriber will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

5.1.4. Taking into account the nature of the processing, Sightengine will assist Subscriber by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of Subscriber's obligation to respond to a Data Subject Request under EU Data Protection Laws. In addition, to the extent Subscriber, in its use of the Services, does not have the ability to address a Data Subject Request, Sightengine shall, upon Subscriber's written request, provide Subscriber with reasonable cooperation and assistance to facilitate Subscriber's response to such Data Subject Request, to the extent Sightengine is legally permitted to do so and the response to such Data Subject Request is required under EU Data Protection Laws. To the extent legally permitted, Subscriber shall be responsible for any costs arising from Sightengine's provision of such assistance.

6. Data Protection Impact Assessment

Upon Subscriber's written request, Sightengine will provide Subscriber with reasonable cooperation and assistance needed to fulfill Subscriber's obligation under the GDPR to carry out a data protection impact assessment related to Subscriber's use of the Services, to the extent Subscriber does not otherwise have access to the relevant information, and to the extent such information is available to Sightengine. Sightengine will provide reasonable assistance to Subscriber in the cooperation or prior consultation with the applicable data protection authority in the performance of its tasks relating to this Section 6 (Data Protection Impact Assessment) to the extent required under the GDPR.

7. Sub-processors

7.1. Subscriber specifically authorizes the engagement of Sightengine's Affiliates as Sub-processors. In addition, Subscriber acknowledges and agrees that Sightengine and Sightengine's Affiliates respectively may engage third- party Sub-processors in connection with the provision of the Services. Sightengine or an Sightengine Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Subscriber Data to the extent applicable to the nature of the Services provided by such Sub-processor.

7.2. Sightengine will make available to Subscriber the current list of Sub-processors for the Services ("**Infrastructure and Sub-processor List**"). Such Sub-processor list will include the identities of those Sub-processors and their corporate location. Subscriber may find the most current Infrastructure and Sub-processor List at https://sightengine.com/policies/subprocessors (under the "Infrastructure and Sub-Processor List" link). Sightengine shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Subscriber Personal Data in connection with the provision of the Services either by sending an email or via the user interface dashboard of the Services.

7.3. Subscriber may object to Sightengine's use of a new Sub-processor by notifying Sightengine promptly in writing within ten (10) business days after receipt of Sightengine's notice. In the event Subscriber objects to a new Sub-processor, as permitted in the preceding sentence, Sightengine will use reasonable efforts to make available to Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber's configuration

or use of the Services to avoid processing of Subscriber Personal Data by the objected-to new Sub-processor without unreasonably burdening the Subscriber. If Sightengine is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Subscriber may terminate the applicable Service Order(s) with respect to only those Services which cannot be provided by Sightengine without the use of the objected-to new Sub-processor by providing written notice to Sightengine. Sightengine will refund Subscriber any prepaid but unused fees covering the remainder of the term of such Service Order following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Subscriber.

7.4. Sightengine shall be liable for the acts and omissions of its Sub-processors to the same extent Sightengine would be liable if performing the services of each Sub-processor directly under the terms of this DPA subject to the limitations set forth in Section 9 (Limitation of Liability) and the Agreement.

8. Covered Affiliates

8.1. The parties acknowledge and agree that, by executing the Agreement, the Subscriber enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Covered Affiliates, thereby establishing a separate DPA between Sightengine and each such Covered Affiliate subject to the provisions of the Agreement, this Section 8 (Covered Affiliates) and Section 9 (Limitation of Liability). Each Covered Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Covered Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Covered Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Covered Affiliate shall be deemed a violation by Subscriber.

8.2. Subscriber that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Sightengine under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Covered Affiliates.

8.3. Where a Covered Affiliate becomes a party to the DPA with Sightengine, it shall, to the extent required under applicable Data Protection Laws, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1. Except where applicable Data Protection Laws require the Covered Affiliate to exercise a right or seek any remedy under this DPA against Sightengine directly by itself, the parties agree that (a) solely Subscriber that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Covered Affiliate, and (b) Subscriber that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Covered Affiliate individually but in a combined manner for all of its Covered Affiliates together (as set forth, for example, in Section 8.3.2, below).

8.3.2. The parties agree that Subscriber that is the contracting party to the Agreement shall, when carrying out an on- site audit of the procedures relevant to the protection of Subscriber Personal Data, take all reasonable measures to limit any impact on Sightengine and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Covered Affiliates in one single audit.

9. Limitation of Liability

9.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA , and all DPAs between Covered Affiliates and Sightengine, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

9.2. For the avoidance of doubt, Sightengine's and its Affiliates' total liability for all claims from the Subscriber and all of its Covered Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Subscriber and all Covered Affiliates, and, in particular, shall not be understood to apply individually and severally to Subscriber and/or to any Covered Affiliate that is a contractual party to any such DPA.

9.3. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Attachments and Appendices.

10. Effect of this DPA

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern.

The parties authorized signatories have duly executed this Data Processing Agreement as of the date set forth below their respective signatures but made effective as of the DPA Effective Date.

Subscriber Entity name:

_____	Sightengine
By:	By:
_____	_____
Title:	Title:
_____	_____
Date:	Date:
_____	_____

ATTACHMENT 1 TO THE DATA PROCESSING ADDENDUM

DESCRIPTION OF PROCESSING ACTIVITIES

Data subjects

Data subjects include the individuals about whom personal data is provided to Sightengine via the Services by (or at the direction of) Subscriber or by Subscriber's end users, the extent of which is determined and controlled by the Subscriber in its sole discretion, and which may include but is not limited to personal data relating to the following categories of data subjects:

1. Prospects, customers, business partners and vendors of Subscriber (who are natural persons)

2. Employees or contact persons of Subscriber's prospects, customers, business partners and vendors (who are natural persons)

3. Employees, agents, advisors, freelancers of Subscriber (who are natural persons)

4. Subscriber's users authorized by Subscriber to use the Services (who are natural persons)

Categories of data

Personal data relating to individuals provided to Sightengine via the Services, by (or at the direction of) Subscriber or by Subscriber's end users, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include but is not limited to personal data relating to the following categories of data:

1. Facial Image

2. Personal photo or video

3. Audio recordings in submitted videos

4. Text messages

5. Usernames

Special categories of data

Subscriber may submit special categories of data to the Service as a part of its Subscriber Data, the extent of which is determined and controlled by Subscriber in its sole discretion, and which is for the sake of clarity personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

Subscriber Personal Data will be processed in accordance with the Agreement and this DPA.

ATTACHMENT 2 TO THE DATA PROCESSING ADDENDUM

SECURITY MEASURES

Sightengine implements and maintains Security Measures at all levels of the organization and at all steps of its operations. Sightengine may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. These Security Measures are in effect on the DPA Effective Date. Capitalized terms used herein but not otherwise defined have the meaning given to them in the DPA.

1. Data Center and Network Security

a) Data Centers

i) **Infrastructure**. Sightengine maintains geographically distributed data centers and stores all production data in physically secure data centers.

ii) **Redundancy**. Sightengine's infrastructure has been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. This design allows Sightengine to perform maintenance and improvements of the infrastructure with minimal impact on the production systems. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications.

iii) **Power**. All data centers are equipped with redundant power system with various mechanism to provide backup power, such as uninterruptible power supplies (UPS) batteries for short term blackouts, over voltage, under voltage or any power instabilities and diesel generators, for outages extending units of minutes, which allow the data centers to operate for days.

iv) **Server Operating System**. Sightengine uses a Linux based operating system for the application environment with a centrally managed configuration. Sightengine has established a policy to keep systems up to date with necessary security updates.

v) **Business Continuity**. Sightengine replicates data across multiple systems to help protect against accidental destruction or loss.

b) Network and Transmission

i) **Data Transmission**. Sightengine uses industry standard encryption schemes and protocols to encrypt data transmissions between the data centers. This is intended to prevent reading, copying or modification of the data.

ii) **Incident Response**. Sightengine's personnel will promptly react to discovered security incidents and inform the involved parties.

iii) **Encryption Technologies**. Sightengine's servers support HTTPS encryption, ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA and for supported clients also perfect forward secrecy (PFS) methods to help protect traffic against compromised key or cryptographic breakthrough. Sightengine's servers use OCSP stapling to harden the presented Certificates. Sightengine uses only industry standard encryption technologies.

2. Access and Site Controls

a) Site Controls

i) **Data Center Security Operations**. All data centers in use by Sightengine maintain 24/7 on-site security operations responsible for all the aspects of physical data center security.

ii) **Data Center Access Procedures**. Access to the datacenter follows Sightengine's Physical Security policy allowing only pre-approved authorized personnel to access Sightengine equipment.

iii) **Data Center Security**. All data centers comply with or exceed the security requirements of SOC2. All data centers are equipped with CCTV, on-site security personnel and key card access system.

b) Access Control

i) "**Access Control and Privilege Management**. Subscriber's administrators must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.

ii) **Internal Data Access Processes and Policies – Access Policy**. Sightengine's internal data access processes and policies are designed to prevent unauthorized persons or systems from getting access to system used to process personal data. Sightengine only provides access to a limited number of authorized personnel. Sightengine requires the use of SSH certificates, unique IDs, strong passwords, two factor authentication where applicable. Access to system is logged to provide an audit trail for accountability.

3. Data

a) Data Storage and Logging. Sightengine stores data in a combination of dedicated and multi-tenant environment. The data is replicated on multiple redundant systems. Subscriber may enable data sharing, should the Services functionality allow it. Subscriber may choose to make use of certain logging capability that Sightengine may make available via the Services.

b) Decommissioned Disks and Disk Erase Policy. Disks used in servers might experience hardware failures, performance issue or errors that lead to their decommission. All decommissioned disk are securely erased if intended for reuse, or securely destroyed due to malfunction.

4. Personnel Security

Sightengine personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Sightengine's confidentiality, privacy and acceptable use policies. All personnel are provided with security training upon employment and then regularly afterwards. Sightengine's personnel will not process Subscriber Data without authorization.

5. Sub-processor Security

Sightengine will only onboard Sub-processors who provide adequate levels of security and privacy to data and scope of services they are engaged to provide. Sightengine maintains an up-to-date list of Sub-processors on its website.