SHORTPIXEL DATA PROTECTION AGREEMENT

This Data Processing Addendum ("**DPA**") is concluded between you ("**Customer**" or "**you**") and ShortPixel and it regulates the data processing activities performed within your use of ShortPixel services. Unless otherwise defined in this DPA or in other applicable agreements (i.e. Terms of Use – the "**Agreement**"), all capitalised terms used in this DPA will have the meaning given to them in Section 2 of this DPA.

1. SCOPE

This DPA applies to the processing operations performed on Customer data for the provision of ShortPixel services, as detailed in Appendix 1 below. In this context, ShortPixel will act as a *data processor* to Customer.

2. DEFINITIONS

The capitalized terms which are not otherwise defined in this DPA shall have the meaning below:

- „**Personal Data**" means any information relating to an identified or identifiable natural person (hereinafter referred to as „Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

- „**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

- „**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- „**Controller**" means the entity determining the purposes and means of the personal data processing;

- „**Processor**" means the entity acting under the authority and instructions of the controller;

- „**Data Protection Authority**" or „**DPA**" means a supervisory authority controlling the processing of personal data because: (a) the Controller or Processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the Processing; or (c) a complaint has been lodged with that supervisory authority;

- „**Data Protection Officer**" or „**DPO**" shall mean the person designated by the Controller or the Processor in compliance with Article 37 of the GDPR;

- „**Transfer of Personal Data**" shall mean any transfer of Personal Data from an entity to another entity. A transfer can be carried out via any communication, copy, transfer or disclosure of Personal Data through a network, including remote access to a database or transfer from one medium to another, whatever the type of medium (for instance from a computer hard disk to a server).

3. OBLIGATIONS OF THE PROCESSOR

3.1. General Obligations

The Processor shall:

- comply with all obligations incumbent upon the data processors, as provided by the GDPR and the Relevant Data Protection Legislation;

- comply with the documented Controller's instructions, in particular without limitation those instructions which are necessary to ensure the Controller is in compliance with the GDPR and the Relevant Data Protection Legislation;

- process the Personal Data solely in order to perform its obligations under the Agreement, only pursuant to the terms and conditions of this DPA and/or in accordance with the instructions of the Controller, except where the Processor is required to have a specific conduct pursuant to GDPR or the Relevant Data Protection Legislation.

- promptly inform the Controller i) of its inability to comply with the provisions of the DPA and/or ii) if, in its opinion, an instruction of the Controller infringes the GDPR or any other Relevant Data Protection Legislation; and

- provide the Controller with the contact details of the Processor's Data Protection Officer, should such Data Protection Officer is appointed in compliance with Article 37 of the GDPR.

3.2. Security and Confidentiality Obligations

The Processor shall preserve the security and confidentiality of the Personal Data and implement all adequate measures to ensure the level of security of the Controller's Personal Data are appropriate.

The Processor undertakes to implement all reasonably necessary and appropriate technical and organizational measures using generally accepted state-of-the-art technology to protect the Personal Data it processes under the Agreement against unauthorized or accidental access, alteration, transmission, disclosure, deletion or destruction.

The Processor shall review and adapt such measures regularly to comply with the state of the art and applicable regulations, namely security measures necessary to ensure the conservation and integrity of the Personal Data processed during the performance of the Contract (for instance to secure the access to computers, to install antivirus, to perform regular backups on removable media and to increase the employees and suppliers' awareness to security measures);

Without limiting the generality of the foregoing, the Processor shall comply with the following obligations and shall ensure that its employees and/or its suppliers will also comply with them:

- The Processor shall process the Personal Data only in accordance with the Controller's instructions and to the extent such processing is necessary to carry out the Processor's obligations in connection with the performance of the Agreement;

- The Processor will not use the Personal Data for any other purposes, nor will the Processor retain this data for any longer than required by the Controller;

- The Processor will only use personnel who: (i) has a need to process the Personal Data in order to fulfill the Processor's obligations under the Agreement, (ii) has entered into a confidentiality agreement; (iii) has received adequate training regarding the protection of Personal Data and (iv) has been informed of any special data protection requirements arising from this DPA and of the limitation of the use of the Personal Data for specific purposes as instructed. The Processor also undertakes to communicate to the Data Controller, upon request, the list of persons so entitled;

- The Personal Data shall not be disclosed to any third party, whether individual or legal person, public or private entity without prior approval of the Controller (in such case the Processor shall maintain a record of any disclosure of Personal Data to a third party and make such report available to the Controller, promptly upon request);

- The Processor is not allowed to make copies or duplicate of the Personal Data without the prior written consent of the Controller, unless such copies or duplicates are necessary for the fulfillment of its obligations under the Agreement.

3.3. Personal Data Breach Notification

The Processor shall notify the Controller of any Personal Data Breach without undue delay and in writing after it becomes aware of such Personal Data Breach. Such notification shall at least contain the following information:

- the nature of the Personal Data Breach including where possible, the data categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

- the name and contact details of the Data Protection Officer or other contact point where additional information can be obtained;

- a description of the likely consequences of the Personal Data Breach;

- a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Processor also undertakes to provide the Controller with reasonable assistance and co-operation to notify the Personal Data Breach to the competent Data Protection Authority and to communicate such Personal Data Breach to the Data Subjects, in compliance with Articles 33 and 34 of the GDPR and any Relevant Data Protection Legislation.

The Processor shall design and implement procedures for managing and reporting such Personal Data Breach to the Controller.

3.4. *Exercise of Data Subjects' rights*

The Processor shall provide the Controller, taking into account the nature of the Processing, with reasonable assistance and co-operation, to allow the Controller to respond (i) to requests presented by Data Subjects for exercising their rights, or (ii) to requests of the competent Data Protection Authorities in relation with the Processing of Personal Data. In particular, the Processor shall implement appropriate technical and organisational measures in order to promptly satisfy in writing, within 5 working days, any request for information from the Controller.

The Processor may only grant access to, correct, delete, block, restrict the Processing of, or communicate to the Data Subject the Personal Data processed on behalf of the Controller in a structured, commonly used and machine-readable format, when instructed to do so by the Controller.

If a Data Subject would send directly a request or a complaint to the Processor, the Processor shall forward this request or complaint to the Controller without undue delay.

3.5. Subcontracting

The Processor may disclose, assign, or otherwise communicate Personal Data to any subcontractor (whether located within the EU or outside the EU) when neccessary for providing the services for the Customer.

The Processor shall impose on its subcontractor by way of a contract or other legal act, the same legal requirements as the Processor itself undertakes under the DPA, in particular the obligation to provide sufficient guarantees in relation with the Processing by implementing appropriate technical and organizational measures. Where the subcontractor fails to fulfil its data protection obligations, the Processor shall remain fully liable towards the Controller for the performance of that subcontractor's obligations.

3.6. Transfers of Personal Data outside the EEA

The Processor undertakes to:

a. only carry out Transfers of Personal Data outside the EEA when neccessary for providing the services to the Customer.

b. ensure that its own subcontractors, the persons acting under the authority or on behalf of the Processor, do not carry out any Transfer of Personal Data concerning Controller's Personal Data information outside the EEA unless required for the provision of the services;

c. if the Processor appoints a subcontractor, located outside the EEA, the Processor shall also ensure, before any Transfer of Personal Data, that the transfer will be carried out in compliance with the GDPR and the Relevant Data Protection Legislation (for instance, by ensuring that the EU Standard Contractual Clauses approved by the EU Commission on February, 10, 2010 (c2010/0593) will be signed by the subcontractor, if the latter is located in a country which does not provide for an adequate level of protection of Personal Data).

4. DOCUMENTATION AND AUDIT RIGHTS OF THE CONTROLLER

The Controller is entitled acces to the relevant documentation regarding audits performed by the Processor. Any issues, errors or irregularities that are identified, and brought to the Processor's attention, will be promptly remedied by the Processor without delay. The Processor will assist the Controller with any data protection audits or controls enforced by a Data Protection Authority or other competent public authority if these audits or controls concern data Processing within the scope of the DPA.

5. RETENTION, RETURN OR DELETION OF DATA

During the execution of the Agreement, the Processor undertakes to implement adequate technical and organizational measures to comply with data retention periods applicable to Controller’s Personal Data processed under the Agreement where requested by the Controller.

Upon termination of the Agreement, the Processor shall at the Controller’s request, either (i) return all Personal Data processed and the copies thereof to the Controller or (ii) destroy all the Personal Data.

6. LIABILITY AND INDEMNIFICATION

Pursuant to the provisions of Article 82 of GDPR, Processor shall indemnify, defend and hold the Controller harmless from any and all any claims asserted by any Data Subject, Data Protection Authority or any third party with respect to a breach of any of the Processor’s obligations under this Agreement, to the extent the Processor is responsible for the event giving rise to any such claim.

7. TERMINATION

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

In the event the Processor is in breach of any of its obligations under this DPA, the Controller may:

a. suspend the transfer of Personal Data to the Processor until the breach is repaired to the Controller’s reasonable satisfaction or the Agreement is terminated; or

b. terminate the Agreement.

BY ADHERING TO THE PROVISIONS OF THE AGREEMENT, the terms of this DPA are also deemed accepted by the Controller and will regulate the data processing activities performed for the scope of the Agreement.

APPENDIX 1

Personal Data Processing activities

Purpose(s) of Processing	Provision of image optimisation services for the benefit of the Customer
Category/ies of Personal Data	Name and surname, e-mail address, images to be processed, IP
Category/ies of Data Subjects	Customers
Duration of Processing operations	During the term of the Agreement

APPENDIX 2

Summary of the Technical and Organizational Security Measures in order to ensure protection of Personal Data

1. **Information Security Program**. ShortPixel will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the ShortPixel Network, and (c) minimise security risks.

2. **Designated Information Security Person**: ShortPixel will designate a designated person to coordinate and be accountable for the information security program.

3. **Main points of the information security measures:**

   a. *User access management:* Acces to Personal Data is only provided to those employees and contractors who have a legitimate business need for such access privileges.

   b. *Network Security*: ShortPixel network will be electronically accessible to employees, contractors and any other person as necessary to provide the services under the Agreement.

   c. *Physical security:* Acces control procedures implemented to prevent unauthorised entrance to Processor's facilities.

   d. *Continued Evaluation*: ShortPixel will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against industry security standards and its policies and procedures.

4. **Other measures described within the content of the DPA**