

# GoPro Processing Agreement

## Data Protection Standard Terms – Processing Agreement

This Appendix (the “**Processing Agreement**”) applies to the way GoPro (hereinafter the “**Processor**”, “**Us**”, “**We**”, “**Our**”) handles personal data and the rights and duties of the Parties in connection to such data. This Processing Agreement forms a part of the Agreement between the Customer (as defined below) and Processor, regarding the Customers subscription to Hosted Services (as defined below) from the Processor (including under a Licence Agreement) (the “[Agreement](#)”).

Terms used in this Processing Agreement that are not defined herein, shall have the meanings defined in the Agreement. All the terms of the Agreement also apply to this Processing Agreement, including all provisions on indemnity, warranty, limitation of liability and damage caps and waivers.

## TABLE OF CONTENTS

1. DEFINITIONS .....	3
2. AUTHORITY .....	5
3. OBJECTIVES OF AND SCOPE OF THE PROCESSING .....	5
4. PROCESSING CUSTOMER PERSONAL DATA .....	6
5. OUR PERSONNEL .....	7
6. SECURITY .....	7
7. ORIGIN OF INFORMATION AND RESPONSIBILITY .....	8
8. SUB PROCESSING .....	8
9. RIGHTS OF DATA SUBJECTS.....	9
10. SECURITY INCIDENTS .....	10
11. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION .....	10
12. DELETION OR RETURN OF CUSTOMER PERSONAL DATA .....	11
13. AUDITS.....	11
15. AMENDMENTS AND NOTICES .....	12
16. GENERAL TERMS AND INDEMNITY DECLARATION .....	13

## 1. Definitions

1.1 In this Processing Agreement, the following terms have the meanings ascribed to them below:

1.1.1 “**Controller**” means the Customer.

1.1.2 “**Assessor**” means an independent party that is, at any given time, tasked by the Processor with assessing and/or certifying the implementation of the Processor’s ISMS (as defined below) and its performance. Information on the assessor and the certificate currently in force can be found on the Our website - [ISMS](#).

1.1.3 “**GDPR**” means Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).;

1.1.4 “**ISMS**” means the Information Security Management System in force for the Processor at any given time. We strive to constantly update and develop Our security measures, to achieve ever-increased integrity of information and promote a culture of awareness and consciousness in the handling of delicate information. The goal is to maximize the security of information while maintaining efficiency in the operation of and pricing of Our products and services. It is the policy of the Processor that its ISMS covers the key-aspects of the operations of the company; software development, the provision of IT services, consulting, hosting and management. When developing and implementing its ISMS the Processor will endeavour to follow the generally accepted industry standards and processes that are the best fit at the relevant point in time. A description of the ISMS (and Our Information Security Policy) that is currently in force can be found on Our website – [ISMS](#).

1.1.5 “**Customer**” has the meaning ascribed to the term in the [Agreement](#). When applicable in this Processing Agreement, the term also applies to; all employees of the Customer, his advisors and other specialists that the Customer tasks with carrying out specific tasks, processes, audits, changes and other development of the Solution, the Service, Custom solution, the Hosted Services or Hosting.

1.1.6 “**Data Protection Laws**” means the data protection legislation of the European Union, in particular the GDPR and Icelandic laws and regulations on data protection in force at any given time. When applicable, the term also refers to other laws and regulations on the use of, retention and storage of, duty to preserve and duty to provide information on personal data and documents containing such data.

- 1.1.7** "Customer Personal Data" means the personal data that the Processor processes on behalf of the Customer in accordance with the terms of the Agreement or in connection with the Agreement. The restrictions and limitations on that processing are described in Article 3.
- 1.1.8** "Processor" means the Processor and its Affiliates.
- 1.1.9** "Affiliate/(s)" of a relevant party, refers to an entity which, directly or indirectly, owns or controls that party, is owned or is controlled by that party, or is under that party's common ownership or control with other parties, where "control" means the power to direct the management or affairs of an entity, and "ownership" means the beneficial ownership of 50% (or, if the applicable jurisdiction does not allow majority ownership, the maximum amount permitted under such law) or more of the voting equity securities or other equivalent voting interests of the entity. Information on Our group of Affiliate companies can be found on [Our website](#).
- 1.1.10** "Sub-Processor" means any individual or legal entity that might be appointed to or contracted by the Processor to carry out a part of the Services that involves processing Customer Personal Data.
- 1.1.11** In this Processing Agreement, the term "Service" is used to refer to the service We provided to the Customer under the [Agreement](#), that can consist of the provision of, and access to, the following:
- a) "Hosted Services" refers to Our hosted and/or cloud-based software Solutions, whereby the Customer gets access to an end-user-licence for Our Products that are installed in Our computer systems of, specially prepared for running the Product. The computer system that the Customer gets access to with the Hosted Service is comprised of: i) an end-user-licence to run the Product, along with regular updates, ii) software operated on the hardware of the computer system, iii) storage space, processors and disks, iv) server software, v) a database system with disks that store the data that the Customer uploads into the computer system, vi) the system software needed to run the computer system, vii) telecommunication lines, and ix) a reserve power station. The Hosted Services and the computer system that they provide access to are in constant development and renewal and change from time to time. The same applies to the specs for storage limits, processing limits and other aspects of the computer system.
  - b) "Hosting". Hosting means a service that is not standard or commercially available, but specifically agreed on by an agreement between the Customer and Us. In instances where a Hosting agreement is in place between the Customer and Us, any reference to the Agreement shall be a reference to the Hosting agreement.

- 1.1.12** “**Security Incident**“ covers both of i) an information security event that occurs when the integrity of the [ISMS](#) may have been breached or the procedures of the [ISMS](#) not followed, and ii) a personal data breach, as that term is defined in Data Protection Laws.
- 1.2** The terms, "**Data Subject**", "**Member State**", "**personal data**", "**processing**" and "**supervisory authority**" have the meanings ascribed to the terms in the GDPR and the Icelandic legislation enacted to implement the GDPR.
- 1.3** Other terms not defined herein shall have the meaning ascribed to them in the Agreement.

## **2. Authority**

Processor warrants that if an Affiliate undertakes any part of the processing of the Customers Personal Data that forms a part of the Services, We will, prior to the processing taking place, ensure that the relevant Affiliate is bound by the same commitments towards the Customer as We are under this Processing Agreement.

## **3. Objectives of and scope of the processing**

- 3.1.** The Processor and the Customer conclude this Processing Agreement alongside the [Agreement](#). Under the [Agreement](#), the Customer orders or subscribes to the Service. According to Personal Data Laws, a part of the service provided by Us are considered processing, because they include storage of data. The Processor itself will not handle the collection, recording, organising, structuring, adaptation, use, disclosure by transmission, dissemination or otherwise make available, align, combine, or restrict access to the personal data that the Customer chooses to upload into Our Products or the Service.
- 3.2.** The Product that the Customer gets access to on the basis of the [Agreement](#) enables the Customer to carry out various different forms of data processing, including processing personal data. These operations or sets of operations are not performed by Us and thus do not constitute processing carried out by Us.
- 3.3.** All data that the Customer uploads into the Product or Service and is stored with Us belong to the Customer. We will not use these data in any way nor transfer them or transmit, unless at the explicit request of the Customer.
- 3.4.** If the Customer specifically requests, it may be that Our employees view a limited set of personal data, for a specific purpose, to carry out a service request. It is also possible that the Customer may seek Our assistance in retrieving personal information or request that We delete personal data when the term of the Agreement expires. Such operations are also considered processing according to Data Protection Laws.
- 3.5.** In view of the foregoing, the processing operations performed by Us as a Processor under the Agreement are very limited in scope and this Processing Agreement reflects this reality.
- 3.6.** According to Data Protection Laws, in particular Art. 28 GDPR, the processing of personal data shall be governed by a contract that meets certain requirements. This

Processing Agreement is intended to set out the rights and obligations of the parties, regarding Customer Personal Data and its processing.

- 3.7.** Certain of Our Solutions enable the Customer to provide access to specified parts of the Customer's program to outside parties, for example to upload data, work on documents, file applications or open cases. Through such access it is possible to disseminate and disclose data, share them, copy and alter. Certain of Our Solutions also offer the possibility of electronically signing documents. All these applications that are offered by these Solutions are forms of processing data. For the avoidance of doubt, it is specifically stated by the Customer (if he uses these applications) and the Processor, that all such processing is carried out by, or according to the determination of, the Customer, for example under access restrictions or procedures decided by the Customer. Processing that is carried out with such application is therefore not carried out by Us, although the tools used are parts of Our Solutions.

## **4. Processing Customer Personal Data**

### **4.1 The Processor:**

**3.1.1.** Will adhere to Data Protection Laws when carrying out the processing of Customer Personal Data.

**3.1.2.** Will only process Customer Personal Data according to documented instructions from the Customer, unless specific processing is required by applicable laws that We (or an Affiliate) are subject to. In such cases We will, to the extent permitted by the applicable law, inform the Customer of the legal requirement before the relevant processing of that Customer Personal Data.

### **4.2 The Customer:**

**4.2.1** Instructs the Processor (and Affiliates) to process the Customer Personal Data as needed to provide the Service according to the Agreement.

**4.2.2** Warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the Processor that instruction and that the Customer has collected the Personal Data according to sufficient legal permissions, lawful consent, and in all manner in accordance with Personal Data Laws.

- 4.3** Schedule 1 to this Processing Agreement contains more detailed information on the subject matter and nature of the Customer Personal Data that the Processor is charged with processing, as required by Para. 3 of Art. 28 of the GDPR. The obligations of the Parties must however always be viewed in the context of the very limited processing that the Processor is tasked with, as described in Art. 2. Schedule 1 is first and foremost for information purposes and intended to give an overview of the processing that the Processor is charged with, but not to increase or decrease the substantive obligations of the Parties. The Agreement and this Processing Agreement contain more detailed provisions on the substance of the processing and Schedule 1 is therefore only intended to be complement those texts.

## 5. Our personnel

All employees of the Processor, advisors, agents, contractors and other service providers (jointly “**Our Personnel**”) who may have access to the Customer Personal Data, are aware of the need to handle such information with care. Our Personnel will under normal circumstances not access or have access to Customer Personal Data, unless in instances where the Customer so requests or if access proves necessary to provide the Service. All Our Personnel are subject to confidentiality undertakings according to their employment agreement. Our Personnel that works on tasks connected to data that are subject to increased confidentiality on the basis of legislation or contract, or due to the nature of the task, execute specific confidentiality undertakings that apply to those tasks. These matters are covered by Our [ISMS](#).

## 6. Security

- 6.1** The Processor has taken measures that aim at ensuring an appropriate level of security for the Customer Personal Data, taking into account; the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks it entails for the rights and freedoms of natural persons. In these matters, We follow the rules and guidance set forth in Art. 32 GDPR.
- 6.2** The level of security varies according to which version of Service the Customer has chosen with the Agreement. We offer a standardised, Hosted Services package, that includes security measures that We consider appropriate for the general needs of a regular customer. We also offer additional Solutions that involve substantially increased security measures. A list of the Solutions on offer and details about what is included in different implementations, at any given point in time, can be found on the Our website.
- 6.3** The Customer has studied the different Solutions on offer and chosen the Service based on his own assessment of what is the appropriate level of security for his needs and to ensure the safety, integrity and confidentiality of the Customer Personal Data.
- 6.4** If the Customer requires additional security measures, in addition to those that the Processor offers as a basic, standard service according to Art. 6.1 and 6.1, or if the Customer requests that Our Solutions or the Service are tailored to implement specific additional information security, in addition to the standardised services chosen by the Customer under the Agreement (for example, if by adding additional applications listed in Art. 32 GDPR) this will be done on the basis of a special contract and a fee negotiated for these additional services and Custom solutions. If there are substantial changes to the nature and type of Customer Personal Data and the Customers need for data security, the Parties will conclude a tailored Hosting agreement to meet those needs.
- 6.5** Our information security is tested regularly and is constantly being developed. That process, as well as the [ISMS](#) in general, is updated regularly to reflect the newest trends in information safety and audited and inspected as deemed necessary by an Assessor. As part of this process, We perform vendor assessments on our service providers, in accordance with the [ISMS](#). We have also implemented a Data Protection Policy that is updated regularly to reflect new technology and best practice. The [Data Protection Policy](#) can be viewed on Our website.

## **7. Origin of information and responsibility for Customer personnel and third party actions**

**7.1** When the Customer tasks his employees, advisors, agents, contractors and other service providers (jointly “Customer Personnel”) to perform changes, amendments, inspections, audits, remove or copy data, or perform other types of processing in connection to the Service, Our Solution, Hosting or Hosted Service, whether the task is performed on Our premises or not, We bear no responsibility for the results of those tasks. If these tasks of Customer Personnel causes damages, loss, injury, harm, impairment or other forms of negative impact, whether on Our interests or on the interests of other users of Our Solutions, the Customer is liable to settle all such claims in full according to the general rules applicable (under tort, contract, equity or otherwise).

**7.2** Certain of Our Solutions enable the Customer to grant access to his environment to specific third parties, or a group of individuals and entities, that meet criteria set by the Customer. Having been granted such access, these third parties can upload documents and data into the Customers environment, open cases, procedures and applications. We are not responsible for the reliability and authenticity of documents, data and information from such sources. The Customer is responsible for ensuring, inter alia by using correct settings and access controls, that such third parties do not get access to the personal data of other Data Subjects.

**7.3** When the Customer utilises outside sources of information or data to automatically categorize individuals, legal entities and groups, that are granted access to the Customers’ environment (or parts thereof), We are not responsible if such information or data proves to be wrong, insufficient or incomplete and lead to third parties being granted the wrong form of access, connection or other forms of Security Incidents. This applies for example if data from national registers, or similar databases, is used to manage which parties get access to the Customers system, and what type of access they get.

**7.4** We will however, in all the instances listed in Ar. 7.1, 7.2, and 7.3, provide assistance to the Customer, and respond appropriately to Security Incidents, in order to facilitate the security of Customer Personal Data, according to Art. 9, **Error! Reference source not found.**, 12, and **Error! Reference source not found.**.

## **8. Sub processing**

**8.1** The Customer authorises the Processor to appoint Sub processors to carry out parts of the Service, according to the procedures and restrictions in this Art. 8.

**8.2** If the Processor intends to appoint a Sub processor, he shall notify the Customer and inform him which part of the Service will be undertaken by the Sub processor. If the Customer does not object to that notice within 7 days of its receipt, he is considered to have approved the Sub processing. If the Customer objects within that time, the Processor shall not share any Customer Personal Data with the Sub processor, until appropriate arrangements have been made to react to the objections of the Customer and those arrangements have been explained to the Customer.



- 8.3** In all instances when a Sub processor is appointed the Processor shall:
- 8.3.1** Before the Sub processor initiates any processing, carry out sufficient due diligence to make sure that the Sub processor can provide the level of protection for Customer Personal Data that the Agreement requires;
  - 8.3.2** Conclude an agreement with the Sub processor that satisfies the requirements of Para 3 Art 28 GDPR, and that ensures that when the Sub processor carries out any processing of the Customer Personal data, he is bound by terms that are in no way less secure than the terms of this Processing Agreement; and
  - 8.3.3** If the Customer so requests, provide him with a copy of the agreement referred to in Art. 8.3.2, when appropriate after commercially sensitive information has been deleted.
  - 8.3.4** If a Sub processor does not comply with his data protection obligations, the Processor remains liable to the Customer for such obligations, on the basis and under the conditions provided for in this Processing Agreement, as if no Sub Processor had been appointed.
- 8.4** The Processor shall ensure that the Sub processor adheres to all obligations under Art. 4.1, **Error! Reference source not found.**, **Error! Reference source not found.**, 9.1, 10.2 and 13.1, as they apply to the processing of Customer Personal Data carried out by the Sub processor, as if he was himself party to this Processing Agreement.
- 9. Rights of Data Subjects**
- 9.1** The Data Protection Laws ensure various rights of Data Subjects, such as the right to access data regarding themselves, the right to rectification, the right to erasure, the right to restrict processing and the right to data portability. Taking into account the limited nature of the processing that We are tasked with, We will provide the Customer with technical and organisational assistance to fulfil the Customers' obligations towards Data Subjects under Data Protection Laws. If that assistance goes beyond what is a normal part of the Service, We will provide such assistance at the hourly rate according to the tariff in force at the time.
  - 9.2** When it is necessary to store information regarding the processing of particular Customer Personal Data (for example what was processed, when, by whom and for what purpose), that has already taken place before the Data Subject requests its erasure, the deletion of the data will take this into account. If a Data Subjects' request for erasure is in conflict with legal requirements to preserve or store data, for example on the basis of laws on official databases and file directories, procedural rules, bookkeeping and accounting rules, or similar reasons, We will consult with the Customer whether and how erasure is to take place.
  - 9.3** We will, without undue delay, notify the Customer of all inquiries We receive from Data Subjects regarding the Customer Personal Data. We will only react to such inquiries in accordance with documented instructions from the Customer, unless legally required to respond directly.

**10. Security Incidents**

- 10.1** If We become aware of a Security Incident that affects the Customer Personal Data, We will, without undue delay, notify the Customer and provide him with sufficient information to satisfy the Customers' obligations to report the Security Incident to the supervisory authority and/or the Data Subject, in accordance with Data Protection Laws.
- 10.2** We will assist the Customer and take such commercially reasonable steps as are appropriate in scope to assist the Customer in investigating, mitigating and remedying the Security Incident. If the Security Incident is not caused by Us, work will be charged at the hourly rate according to the tariff in force at the time, unless the Customer and the Processor specifically agree otherwise.
- 10.3** If the Customer notifies a Security Incident relating to the Service and the notice proves based on untrue or unsubstantiated assertions of Customer Personnel (or others that the Customer is responsible for), the Customer is liable to pay for the work of Our Personnel that results from the notice, at the hourly rate according to the tariff in force at the time.
- 10.4** We have in force a meticulous procedure for handling matters relating to Security Incidents that can arise and maintains precise logs on actions taken in such cases. These procedures fall under Our [ISMS](#) and are evaluated periodically by an Assessor.
- 10.5** Our Solutions may log, timestamp and otherwise keep track of instances when Customer Personal Data is shared and disseminated during the Customers' use of the Service. If the Customer request such logs to be kept, he is the Controller of that processing and charges us to undertake that processing according to his instructions. If the Customer does not request such logs to be kept, We will still keep them and be the Controller for the processing, as such logs are intended to increase the transparency and traceability of the use of Products and personal data processing involved in their use. We agree to provide the Customer with information from these logs as needed to investigate Security Incidents, unless the rights of other users, customers, their data or Our data security and data protection obligations restrict us in doing so.

**11. Data Protection Impact Assessment and Prior Consultation**

- 11.1** The Customer is responsible for conducting appraisals of how processing will affect data protection, cf. Art. 35 GDPR. The Customer is also responsible for carrying out prior consultation with supervisory authorities if it is his assessment that the processing can involve high risk. We will provide the Customer with reasonable and appropriate assistance in carrying out impact assessments and prior consultation. That assistance is limited to the processing that We are charged with as a part of the Service and shall reflect the limited scope of that processing. If the Customer requests technical and professional assistance from Us that exceeds what the Service entails, such assistance is provided at an hourly rate according to the tariff in force at the time.
- 11.2** We have conducted Our own risk assessment and evaluated Our systems for potential weaknesses. That assessment is a part of the procedures that are independently audited and appraised by an Assessor according to the detailed and precise requirements of the ISMS.

**12. Deletion or return of Customer Personal Data**

- 12.1** Subject to Art. 12.3 and 12.4, We will, without undue delay after the term of the Service is over, delete all Customer Personal Data that We may have been provided with.
- 12.2** Despite Art. 12.1, logs of processing and meta-data on (for example) who has processed a document and shared it, for what purpose, in what way and at which time, will not be deleted. There can be a need to preserve such logs and meta-data for a longer period due to the rights of the Data Subject they relate to, the interests of the Processor and/or the interest of the Controller. Such logs and meta-data will be deleted as soon as there is no longer a need for their retention. If the Customer utilises Hosted Services, has a tailored Hosting agreement, or uses similar services provided by Us; backups of the Customers' system are made in accordance with the terms of the relevant service. The frequency of, and storage time of backups is decided by Our retention policy. As a result of the limited storage time of each backup, all stored Customer Personal Data gets automatically deleted over time, after the term of the Service is over. If the Customer feels that copies of the Customer Personal Data needs to be deleted sooner, the Parties will agree on a price for that service.
- 12.3** If the Customer wants Us to return a complete copy of all Customer Personal Data that We have received, by secure file transfer, and delete all other versions, the Customer shall request so in writing no sooner than two months and no later than 7 days before the Subscription Term for the Service is over. Such copying will be charged in accordance with the tariff in force when We receive the request.
- 12.4** When required by law, We will retain Customer Personal Data for the time demanded by the relevant legal obligation. In such instances We will keep the relevant data confidential and secure and only process it as legally required to.
- 12.5** In cases where there is reasonable doubt as to whether particular data is Customer Personal Data or belongs to another party, We reserve the right to (at Our own choice) either seek advise or an opinion from competent authorities before deletion takes place, or to only delete the relevant data on the condition that the Customer signs a contractual obligation to indemnify and hold Us harmless from any resulting claim or dispute, in a form acceptable to Us.

**13. Audits**

- 13.1** We will, at the Customers request, make available to him the information he requires in order to demonstrate that obligations under this Processing Agreement are met. If there is a particular need for it, We will permit an audit of Our processing of Customer Personal Data, subject to Art. 13.2, 13.3 and 13.4.
- 13.2** Audits shall only take place when there is an actual need and it cannot be sufficiently demonstrated that obligations are met by providing documentary evidence and information. Audits shall only inspect the limited processing that We carry out on the Customer Personal Data. An audit shall only be performed by an auditor approved by Us, such approval not to be unreasonably withheld.
- 13.3** If an audit proves necessary, the Customer shall give Us reasonable notice and make all reasonable endeavours to avoid causing any damage, injury, harm or disruption to

Our premises, equipment, personnel and business. The Customer is liable for all damages, loss, injury, harm, impairment or other forms of negative impact that result from an audit.

**13.4** We reserve the right to restrict the scope of audits as needed to protect the security and integrity of the information and personal data of other users of the relevant system or service. If We consider it obvious that an audit or information request is excessive and that the amount of information and data exceeds what is reasonably required for the purposes of the Customer, We will notify the Customers contact. If the Customer wants to pursue the information or audit request nonetheless, We will charge a premium on top of the hourly fees incurred.

**13.5** If an audit, or work needed to prepare and compile information for the Customer, leads to cost for Us, the Customer will reimburse that cost. If services or assistance from Our personnel is needed in carrying out an audit, or work is required in preparing and compiling information for the Customer, the fee for that service is charged at the tariff in force at the time. Audits shall only take place during normal working hours, unless the Customer and the Processor specifically agree otherwise.

#### **14. Restricted transfers**

**14.1** The Processor will not transfer Customer Personal Data to third countries or international organisations, unless under an obligation to do so under applicable law or the orders of a court or public authority with the mandate and jurisdiction to demand such transfer. A description of the Hosted Service environment can be found on Our web.

**14.2** If, during the term of the Agreement, the Processor intends to change that policy and transfer data, the Customer will be notified in advance. If the Customer does not object to that intention within 7 days of receiving the notice he is considered to have approved of the intended restricted transfer. If the Customer sends a reasonable objection within that time, the Processor will not transfer any Customer Personal Data to third countries or international organisation, until reasonable measures have been taken to react to the Customers concerns and these measures have been explained to the Customer. The Processor will not transfer personal data outside the European Union unless there is a contract in place, between the Processor and recipient that satisfies the requirements of Data Protection Laws and binding corporate rules are in place to ensure the security of Customer Personal Data.

#### **15. Amendments and notices**

**15.1** If changes are made to Data Protection Laws that the Processor feels require amendments to this Processing Agreement, the Processor can suggest these amendments by sending a notice to the Customers contact party. If the amendments are non-material and aimed at increasing the rights or security of the Customer, without placing additional obligations or burdens on him, the will enter into force upon receipt of the notice. If not, the suggested amendments will be mutually agreed on by the Parties without undue delay.

**15.2** All notices, requests and formal correspondence based on or connected to this Processing Agreement shall be deemed sufficiently given if sent by e-mail to the address of the contact of the relevant recipient Party listed below and its receipt is

digitally confirmed. Notices are also validly given if they are sent in a different manner and their receipt can be confirmed. To confirm receipt it is sufficient to demonstrate that registered mail was delivered, or a service processor confirms delivery, at the recipients registered address,

**15.3** The contact party of the Customer is listed in Schedule 1.

**15.4** The contact party of the Processor is listed in Schedule 1.

**16. General terms and indemnity declaration**

**16.1** The Customer undertakes and commits himself to indemnify Us, Our Personnel, Our officers and directors, stockholders, affiliates, subcontractors and customers from and against all allegations, claims, actions, suits, demands, damages, liabilities, obligations, losses, settlements, judgments, costs (including legal costs) and expenses, which arise out of, relate to or result from Us (or other indemnified parties) adhering to instructions from the Customer regarding Customer Personal Data.

**16.1.1** This indemnification does not apply to instances where We (and other indemnified parties) had to be aware that instructions were unlawful and that following them would result in damages.

**16.1.2** It is further stated, for the avoidance of doubt, that this indemnification does not apply in instances where a decision of a competent authority to impose a penalty is based Our culpability. In such instances the settlement of penalty amounts between Us and the Customer shall be based on general principles of law.

**16.2** The Parties submit to the choice of law and jurisdiction stipulated in the [Agreement](#), with respect to any dispute or claims however arising under this Processing Agreement.

**16.3** If there are any divergences or discrepancies between the terms of this Processing Agreement and the [Agreement](#), the terms of the [Agreement](#) shall prevail.

**16.4** All terms of the [Agreement](#) that are not specifically derogated from herein, also apply to this Processing Agreement, including but not limited to all the [Agreements'](#) provisions on termination, confidentiality, and limitations of liability and damages.

In confirmation of all the above:

**On behalf of the Processor**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

## Schedule 1

**DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA**

This Schedule contains certain details of the processing of Customer Personal Data that the Processor is charged with, as required by Art 28(3) GDPR

**Customer contact party**

Name:

Address:

Recipient: \_\_\_\_\_,

e-mail address:

Customer can change contact parties by sufficiently notifying the Processor.

**Processor contact party**

Name:

Address:

Recipient: \_\_\_\_\_,

e-mail address:

the Processor can change contact parties by sufficiently notifying the Customer.

*Subject matter, scope and duration of the processing of Customer Personal Data*

The scope and subject matter of the processing is described in Art. 2 of the Processing Agreement and is determined by the nature of the Services described in the Agreement

The duration of the processing is the same as the term of the Agreement.

*The nature and purpose of the Processing of Customer Personal Data***[INS description]**

*The types of Customer Personal Data to be processed*

**[INS description]**

*The categories of Data Subjects to whom the Customer Personal Data relates*

**[INS categories of data subjects]**

on behalf of the Processor

on behalf of the Customer

By signing this Schedule, the Customer agrees to and submits to all terms of the Processing Agreement (and the [Agreement](#)). With each payment of an invoice from the Processor, that commitment is repeated.