GoPro´s Data Protection Policy

1. PURPOSE

In business operations such as GoPro´s, it is inevitable that companies need to collect various forms of information and data. These data may involve natural persons, which can, in some instances, be identifiable, or the data capable of being traced to them. It is GoPro´s policy to collect only such personal data as is necessary for its operations, in accordance with law and in a transparent manner and with respect for the rights of data subjects. When appropriate, consent for the processing of data will be sought. GoPro is intently focused on data protection and the purpose of this Data Protection Policy is to facilitate that personal data of employees, customers, and other stakeholders is treated with respect and held in confidence. The Policy is intended to clarify; i) which data GoPro collects, ii) for which purposes, iii) how the data are used, iv) which measures GoPro takes to promote the security and protection of data, and v) which rights the data subjects enjoy. It is the core-aim of the Policy that processing of personal data is carried out in light of the principles of Art 4.

In this policy, GoPro will also be referred to as "**We**", "**Our**", "**Us**", or the "**Company**")

2. DATA SUBJECT TO THIS POLICY

2.1. When we act as a controller:

In connection with Our operations, the services that We provide and the products We market, We and Our Affiliates (as defined below), get access to various categories of information and data. This includes data that can be considered personal data within the meaning of Data Protection Laws (as defined below). This Policy applies to such data and Our handling of it.

2.2. When we act as a processor:

In other instances, information and data on individuals could be stored on Our systems, and thus, technically, held by Us, even though We do not collect that data nor determine the purpose and means of processing it. By way of example, this applies to data that Our Customers upload into their systems that are hosted or backed up by Us, and when data is uploaded into those systems by third parties that the Customers provide access to. In these instances, We are not the controller of the data, but can be considered a processor. Data such as these fall under the Processing Agreement in force between Us and the relevant Customer. When appropriate, the Provisions of this Policy will be taken into account to facilitate careful and respectful treatment of personal data.

2.3. Our software used in the processing of others:

When Our software and solutions are installed, run and hosted by Our Customers, We are neither a controller nor a processor for data that are stored and processed with the software.

3. DEFINITIONS:

"**ISMS**"	refers to the Information Security Management System We have in force 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 Our policy that the 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 Our ISMS We 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. You can also view the certificates in force at any given time here.
"**Data Protection Laws**"	refers to Icelandic laws and regulations on the protection of personal data, as in force at any given time, and, as applicable, the legislation of the European Union on the protection of personal data, in particular the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016). When the context provides for it, the term also covers legislation and regulations regarding the handling of, storing of, duty to preserve, duty to deliver, and duty to provide information on, personal data and documents containing such data.
"**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 parties 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.

"Delicate information"	are personal information that are, due to their nature, particularly delicate because they relate to fundamental rights and freedoms, merit specific protection, or their processing can create significant risks to the fundamental rights freedoms of the data subjects. By way of example, these can be data that relate to race, ethnic origin, political opinions, religious beliefs, health data, sexual orientation and similar matters.
"**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 (as further elaborated on in the ISMS), and ii) a personal data breach, as that term is defined in Data Protection Laws.

The terms, "**Data Subject", "Member State", "personal data", "processing",** and **"supervisory authority"** have the meanings ascribed to the terms in the applicable Data Protection Laws.

4. PERSONAL DATA PROCESSING PRINCIPLES

When processing personal data, We will, to the extent possible, adhere to the following principles. These principles shall also be used to clarify and construe other parts of this Policy.

4.1. Personal data are collected in a lawful manner and processed in a fair and transparent way.

4.2. Personal data are collected to serve a legitimate purpose and only processed in connection to that purpose, and/or according to legal requirements or archiving purposes.

4.3. Personal data shall be correct, accurate and sufficient for the processing they relate to. When it possible to do so with reasonable and proportionate means, the accuracy and validity of data will be authenticated.

4.4. We do not collect more personal data then is reasonably needed to achieve the purpose behind their processing.

4.5. Personal data is not stored longer then needed to achieve the aim behind their processing, or according to legal requirements and archiving purposes compatible with that aim.

4.6. The confidentiality of personal data shall be preserved. Technical and organisational measures shall be taken with the aim to achieve a level of security that is appropriate, taking into account the state of the art, costs of implementation, the nature, scope, context and purposes of the processing of the personal data.

4.1. THE PURPOSE FOR COLLECTING PERSONAL DATA AND THE USE OF SUCH DATA

4.2. When is personal data collected

The purposes for collecting personal data are different and depend on the type and categories of data. For example, We collect personal data that concerns Our employees to be able to correctly perform the company´s duties under the employment relationship. We may collect, or be provided with, personal data regarding contacts and employees of Our Customers and Users, or potential Customers and Users, in connection with providing them with services and solutions, or in the purpose of entering into an agreement on the provision of services and solutions. We may also collect certain personal data in connection with enquiries, or service requests, that We receive, the use of Our websites or other Products and Solutions.

4.3. Lawful grounds for processing personal data

We will only collect and process personal data as permitted by law. All collection of personal data will be based on one of the following grounds:

Consent When the basis of intended processing is the consent of the data subject, no processing will take place until that consent is in place in a satisfactory form.

Agreement If the processing of personal data is based on an agreement, or is a step needed in order to enter into a contract at the data subjects' request, the processing should be justifiably required in the context of the performance of the agreement or in the process of concluding the agreement.

Legal obligation If the processing of personal data is based on a legal requirement or obligation that We are subject to, or the orders of a court or administrative body of competency, We will, to the extent practicable, take into account the principle of proportionality and, unless it goes against the purpose of the processing or a legal obligation, notify the data subject about the nature and scope of the processing.

Necessity If the purpose of the processing is to safeguard Our important legitimate interests or those of a third party, the scope of the processing shall be limited to what is necessary and, unless it goes against the purpose of the processing, the data subject shall be informed about the purpose, scope and nature of the processing and informed about the rights of data subjects.

4.4. We use personal data for the following purposes

a) **To perform contractual duties.** This applies to i.a. payroll processing and other payments to employees, contractors and advisors and other forms of remuneration to them. This also applies to such use as regular contact with Users´ contacts.

b) **To provide services, improve services and develop them further**. This could for example apply to various information and inquiries that We receive in connection to Our services and solutions, the frequency and type of certain operations and similar information. Usually such information on use of software is not personally identifiable, although that cannot be ruled out.

c) **To ensure the logging and preservation** of communication and facilitate more efficient resolution of inquiries and service requests.

d) Data from cookies are used **to improve the functioning** of websites and to make their use more personal and convenient.

e) Personal data may be used in the interest of the data subject, to make his use of Our Solutions more efficient and easy, for example by auto filling out certain documents or fields.

f) **For business purposes** such as to assist in the strategic planning, development of products, market research, to improve services, to identify patterns of use, assess efficiencies etc.

g) As We deem necessary **to comply with legal obligations** and instructions from competent authorities.

h) As We deem necessary **to protect** Our **operations**.

We do not use personal data for other purposes, unless with the consent of the relevant data subject.

4.5. How and when personal data is shared

We generally do not share personal data. That may however occur in accordance with the following:

a) To Affiliates to use for purposes outlined in this Data Protection Policy.

b) To service providers that can be considered third parties, in connection with purposes outlined in this Data Protection Policy, such as hosting, storing, processing payments, auditing and other ancillary services necessary for Us to carry out Our operations and render Our main services.

c) As We deem necessary to: (a) comply with laws and regulations, (b) comply with official requests from competent authorities, (c) to adhere to contractual terms in a specific instance, and (d) to protect Our operations, the rights and security of Our personnel and Customers.

d) For other purposes with the consent of the data subject.

e) If We and/or Affiliates take part in a restructuring, merger, acquisition or a similar process, personal data will be shared if necessary, but confidentiality will be ensured.

4.6. Transfer across borders

We do not transfer personal data to third countries or international organisations outside the EEA, unless such transfers are a legal obligation, in accordance with the instructions of a court or tribunal of competent jurisdiction, or according to official requests of competent authorities. If We alter this policy, data subjects will be notified in advance (unless they cannot be reached or if notifying them would involve disproportionate effort). We will not transfer personal data outside the EEA until a contract regarding the transfer and the processing that will take place has been concluded that satisfies the requirements of Data Protection Laws and binding corporate rules have been concluded that ensure the security of personal data.

To the extent that Data Protection Laws permit, and after all conditions on storing and transferring personal data have been met, We could opt to store certain personal data in another Member State where We have offices or other facilities.

5. RIGHTS OF DATA SUBJECTS

Information rights Data subjects have the right to know whether their personal data is collected and processed by Us. Data subjects also have the right to information on the purpose of the processing, who has access to their data, how long the data will be stored (or according to which criteria the storage period is determined) and the origin of the data.

Right to rectification Data subjects have the right to request that inaccurate or wrong personal data is rectified and, taking into account the purpose of the processing, to have more accurate and complete data filed when data is insufficient.

Right to erasure and to restrict processing

Data subjects have the right to obtain the erasure of personal data and the restriction of the processing of personal data, when legal conditions are met.

Right to portability Data subjects have the right to receive personal data concerning them on an appropriate format and to transmit such data as they wish, when legal conditions are met.

6. MEASURES TO PROMOTE LAWFUL PROCESSING AND ACCURACY OF DATA

6.1. Measures implemented in Our ISMS

We implement key measures relating to the processing of personal data in Our ISMS, with the goal of making processes aimed at information security and data protection harmonious and in order to form a comprehensive response and management system.

6.2. Notices to data subjects

We will, when it is compatible with the purposes and grounds for processing, notify the data subject that his personal data is collected and process. The form of the notice will differ from case to case. For example, employees are informed about the processing of their data in their employment contract and the processing is an integral part of the nature of the employee/employer relationship and required by applicable laws.

6.3. Informed consent

When the collection and processing of personal data is not based on a request of a data subject, on an agreement with the data subject, necessary to satisfy a legal requirement, or necessary to protect legitimate interests, We will seek the consent of the data subject. We will inform those data subjects who grant their consent about their right to withdraw their consent at any time. The data subject will also be informed of its rights according to this Data Protection Policy and Data Protection Laws.

6.4. Accuracy and corrections

When personal data is collected efforts should always be made to have them as accurate and correct as possible. When a data subject so requests, inaccurate personal data shall be rectified without undue delay. When it is compatible with the purpose of the processing, the data subject shall have the right to request that incomplete data is completed or further elaborated.

When it is practicable, data shall be updated when the occasion arises. If data has proven wrong or inaccurate, it shall be deleted once it has been corrected.

If data has been shared before it is rectified or deleted, this shall be notified to the recipients, unless notifying constitutes a disproportionate burden.

Only employees that need to do so in the course of carrying out their jobs, for the purposes of processing, shall have access to personal data. Others shall not have access to change, amend, alter or delete personal data, or processing them in any other way.

6.5. Processing in accordance with a specific purpose

When decisions are taken regarding which parties are granted access to personal data and how such data is processed, care should be taken to make sure that such decisions reflect the purpose behind collecting and processing the data in question and that all handling of the data is compatible with that purpose.

7. SECURITY OF PERSONAL DATA

No data transfer is perfectly safe and no data storage is a hundred per cent secure. We endeavour to protect personal data as possible and put a great deal of ambition into measures to achieve that aim. We use realistic, operational, technical and organisational measures that are regularly reviewed and updated with respect to security, efficiency and feasibility. The following measures also form a part of Our ISMS where they are described in more detail.

7.1. Organisational and operational measures to increase security of personal data

Our ISMS. We implement operational protocols as part of Our ISMS, aimed at making Our information security and data protection harmonious and form a comprehensive response and management system for information and personal data. Measures described in this Article 8.1 are a part of those ISMS protocols.

a) **Training and corporate culture.** Our personnel familiarize themselves with the company´s Data Protection Policy and ISMS. They get training and education in information and data security that is tailored as appropriate to their position and responsibility. It is emphasised that Our corporate culture is one of awareness and reflects the need for confidentiality, responsibility and care in the handling of all information. Staff training is categorically registered and it is regularly reviewed whether additional presentations or courses are required. Our personnel, advisors and others that get access to personal data from Us are bound by contractual obligations of confidentiality. Personnel that handle tasks connected to delicate information, or data where additional confidentiality is required, under specific legislation or according to the nature of the task, sign additional confidentiality undertakings that apply to those tasks.

b) **Safe zones.** Our offices are defined as a safe zone. All doors to the offices are locked and entrance guarded by a security system. Only personnel have keys and access codes. Customers, advisors and other guests are only allowed access to the offices if escorted by an employee responsible for them while they are on the premises. The employee shall register the name of the guest and the time of arrival and departure. Guests shall be authenticated by a security-pass.

c) **Clear desk and blank screen policy.** If Our personnel leave their workstation they are to make sure that no personal data is visible on surfaces or screens. Computers and other equipment with screens shall be configured to automatically display a locked screensaver if they are not used for a period of time.

d) **Deletion, destruction and retention periods.** Before paper, disks or other storage media and equipment that contains personal data is destroyed, sold, reused, or thrown away, all personal data must first be securely deleted.

e) **Remote work and work on own devices.** Personnel who work with personal data remotely, on a laptop, in smart phones, transport them on usb-sticks or by other similar means, are informed that personal data may only be transported from Our offices in accordance with the rules of the company´s ISMS. Our personnel is aware

that particular care must be used when connected devices are used to work on personal data outside of Our offices, especially in public. Our personnel are permitted, after seeking prior approval and in accordance with the ISMS, to work using their own devices. All data and information that are saved on, transferred through or worked on in own devices, remain Our property at all times and We retains full control and rights over all such data and information. Permission to use own devices is only granted when the devices have the technical requirements necessary to make sure the sufficient safety of personal data.

7.2. Technical measures to protect and guard personal data

Our ISMS. We implement technical measures as part of Our ISMS, aimed at making its information security and data protection harmonious and form a comprehensive response and management system for information and personal data. Measures described in this Article 8.2 are a part of those ISMS protocols.

a) **Access control.** Access to systems, portals and databases owned by Us are generally controlled and locked, unless access control is obviously not necessary. Access codes are only provided to personnel that have a need for access to a particular system, portal or database due to work tasks. Logs are kept to record which personnel have access to which systems, portals and databases.

b) **Passwords.** Personnel are not permitted to provide others with their passwords. It is not permitted to share passwords through any media. If there is any suspicion that a password has been compromised, it shall be changed without delay.

c) **Copying policy**. Our Copying Policy is defined in Our ISMS.

d) **Data Retention policy**. Our Data Retention Policy is defined in Our ISMS.

7.3. Response to Security Incidents

If a Security Incident arises, clear work processes are followed. These processes are regularly reviewed and updated to facilitate efficient and expedient response to incidents.

A Security Incident can entail that: 1) Confidentiality of personal data is breached and an unpermitted disclosure takes place or a party that is not permitted to access data receives them, 2) data becomes inaccessible, or 3) personal data is altered or tampered with.

If a Security Incident arises, We follow the ISMS and, without undue delay, take measures that are appropriate in scope and scale, to investigate the incident, minimize any damage and rectify the situation. We have a detailed procedure for logging measures and handling matters relating to Security Incidents. Our action plans are among the aspects of the ISMS that are regularly evaluated and certified by independent experts.

If a Security Incident arises, We report the incident to the appropriate supervisory authority without undue delay after the company first becomes aware of the irregularity, unless it is

unlikely to result in a risk to the rights and freedoms of the data subjects involved. Such reports follow a fixed procedure and meticulously structured forms.

In instances where a Security Incident leads to a high risk to the rights and freedoms of data subjects, We notify the data subjects directly, unless appropriate measures have been made that eliminate that risk. Such reports follow a fixed procedure and meticulously structured forms.

8. GENERAL

8.1. This Data Protection Policy is subject to changes. If intended amendments to the Policy are substantial they will be notified specifically. Smaller changes will be implemented into the Policy available on Our website.