QBNK Data Processing Agreement (DPA)

Version Dec. 20, 2022

1 Applicability of this Agreement

1.1 To the extent that and subject to;

a) QBNK Company AB ("Processor"), org. no. 556653-3070 and the Customer identified in the Order Form (the "Controller") have entered into an agreement, with a set of appendices thereto (collectively the "Agreement"), regarding the provisioning of certain Product and services to from Processor to Controller;

b) Parties have not entered into another alternative Data Processing Agreement; and

c) Controller, or another party on Controllers behalf, have uploaded personal data to the Product, this Data Processing Agreement (or as may be referred to Data Processing Addendum), ("DPA") is hereby entered into by the Parties on the same date as the execution of the Agreement.

1.2 Processor and Controller are individually referred to as "Party" and jointly as "the Parties".

2 Background

2.1 As set out in the Agreement QBNK will provide a cloud-based service for managing digital assets in the form of images, video, audio or other digital files. Under such Agreement, Processor may process personal data on Controller's behalf.

2.2 According to Applicable Data Protection Legislation, see clause 3.2 below, the processing of personal data carried out by a data processor on behalf of a data controller shall be regulated by an agreement. The Parties have consequently entered into this DPA.

2.3 The purpose of the DPA is to ensure that Processor's processing of personal data on behalf of Controller is conducted in accordance with Applicable Data Protection Legislation, decisions by authorities and Controller's instructions.

2.4 The DPA is a separate agreement that also constitutes an appendix of the Agreement. In the event of conflicting provisions, the DPA shall be given priority.

3 Definitions

3.1 Unless otherwise stated all words and definitions used with capital letters in this DPA shall have the same meaning as set out in the Agreement.

3.2 "Applicable Data Protection Legislation" means 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 ("GDPR") and laws implementing or supplementing the GDPR (including, when applicable, binding guidance, opinions and decisions published by supervisory authorities, court or other competent authority) applicable to the processing of Personal Data under this DPA, and as amended or supplemented

during the term of this DPA.

3.3 “Data Subject” means the natural person whose personal data is being processed.

3.4 “Personal Data” means any information relating to an identified or identifiable person that Processor processes on behalf of Controller.

3.5 “Processing” or “Process” means 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;

3.6 “Sub-processor” means a natural or legal person, public authority, agency or other body engaged by Processor to process personal data.

3.7 Terms and wording relating to personal data and personal data processing, and that begin with a lower-case letter, e.g. “personal data controller”, “data processor”, “personal data breach”, etc., shall be assigned the meaning given them in Applicable Data Protection Legislation.

4 Obligations and Instructions

4.1 Processor undertakes to only Process Personal Data on behalf of Controller in accordance with the Agreement, the DPA and according to prevailing documented instructions from Controller.

4.2 Controller’s instructions to Processor regarding the nature, purpose and duration of the Processing, the type of Personal Data and categories of Data Subjects are specified in Appendix 1 of the DPA.

4.3 When Processing Personal Data, Processor shall comply with Applicable Data Protection Legislation and with the formal opinions and recommendations of the supervisory authority concerned. The Parties agree that the DPA should be adjusted if required owing to Applicable Data Protection Legislation.

4.4 Processor shall inform Controller if Processor has inadequate or inaccurate instructions regarding Processor’s Processing of Personal Data, or if Processor suspects or discovers that Controller’s instructions fail to comply with Applicable Data Protection Legislation.

5 Security, etc.

5.1 The Product is supplied “as is,” and QBNK makes no warranty or representation (whether express or implied) that the Product will be free from error, uninterrupted or about the accuracy or fitness for any particular purpose. When Processing Personal Data, Processor shall adopt appropriate technical and organizational measures to ensure a level of security that is appropriate in relation to the level of risk, and to protect Personal Data from unauthorized or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to such Personal Data. Under all circumstances, Processor shall implement the measures specified in Appendix 2 of the Agreement.

5.2 Processor shall without undue delay inform Controller in writing of any suspicion of or actual personal data breach that may lead to unintentional or unlawful destruction, loss or modification, or to unauthorized disclosure of or unauthorized access to Personal Data.

5.3 Processor shall provide Controller with the following information in the event of a personal data breach:

a) a description of the nature of the personal data breach, categories of and the approximate number of Data Subjects affected, as well as the categories of and approximate number of personal data entries affected;

b) the name and contact details of the data protection officer or other contact from whom further details can be obtained; and

c) a description of the measures taken or proposed by Processor to address the personal data breach, including measures to mitigate its potential adverse effects.

5.4 When Processing Personal Data, Processor shall assist Controller in meeting its obligations in relation to data protection impact assessments, prior consultations with the supervisory authority concerned and the implementation of appropriate technical and organizational measures, to the extent required by Applicable Data Protection Legislation. If such effort requested from Processor is significant, Processor shall have the right to invoice Controller for such effort on a time and material basis, provided Controller has been notified thereabout before Processor commencing such chargeable work.

6 Confidentiality

6.1 When Processing Personal Data, Processor and those individuals working under the direction of Processor shall treat such data as confidential. Individuals working with Processor who are authorized to Process Personal Data shall enter into a separate confidentiality agreement or be informed that they have a duty of confidentiality under legislation or agreements.

6.2 Processor's duty of confidentiality regarding Personal Data extends beyond the duration of the DPA. In all other respects, Processor's duty of confidentiality shall be governed by what is stated in the Agreement between the Parties.

7 Surrender of Personal Data

7.1 For cases where Data Subjects, the supervisory authority concerned or other third parties request information from Processor that relates to the Processing of Personal Data, Processor shall refer to Controller. Unless required by law, Processor may not surrender Personal Data or other information about the Processing of Personal Data without explicit instruction from Controller.

7.2 Processor shall immediately inform Controller of any contact with the competent supervisory authority regarding, or that may be significant to, Processor's Processing of Personal Data. Processor is not entitled to represent Controller or act on Controller's behalf in contact with the competent supervisory authority.

7.3 Processor shall without undue delay assist Controller in relation to a request from a Data Subject regarding subject-access or the amendment, deletion, blocking or transfer of Personal Data, including by providing all relevant information and documentation, to the extent required under Applicable Data Protection Legislation. If such effort requested from Processor is significant, Processor shall have the right to invoice Controller for such effort on a time and material basis provided Controller has been notified thereabout before Processor commencing such chargeable work. Processor shall not carry out any measure that results in Controller being regarded as acting in breach of Applicable Data Protection Legislation.

8 Sub-Processors

8.1 Controller shall own and retain all IPRs in the Customer Data that is entered into the Product by Controller pursuant to the Agreement. Processor is hereby granted a general authorization to engage the services of a Sub-processor to fulfill Processor's obligations under the Agreement, provided that:

a) Processor informs Controller of the intention to use or replace a Sub-processor in due time before such sub-processor is enlisted, and

b) the Sub-processor via a sub-processor agreement with Processor is subject to the same data protection obligations as set out in the Agreement and above all provides adequate assurances to implement appropriate technical and organizational measures in such a way that the Processing satisfies the requirements in Applicable Data Protection Legislation.

8.2 A list of the Sub-processors engaged and by Controller approved Sub-processors for Processing of Personal Data is provided in **Appendix 1** of the Agreement.

QBNK may unilaterally vary these Sub-processors, from time to time, by notice in writing to Customer. If Customer does not object to such modification within fourteen (14) days, such alteration of Sub-processor(s) shall be considered approved and added (or if applicable removed) to the listed sub-processors in Appendix 1 to this DPA. If Customer during the aforementioned fourteen (14) day period gives notice in writing that it objects to such changes, Parties shall seek to find an alternative set-up that Customer approves. If it is not possible for parties to find a mutually acceptable Sub-processor, QBNK shall have the right to terminate the Agreement with 3 months written notice (during which QBNK may not share Personal Data with sub-Processors other than the ones approved in Appendix 1 to this DPA). If the Agreement is terminated pursuant to this clause, QBNK shall refund Customer pro rata for any prepaid remaining portion of the Term.

8.3 Processor shall ensure that Controller is aware of which Sub-processors are Processing Personal Data by providing, and at Controller's request complete, accurate and up-to-date information regarding all Sub-processors, specifying the following information for each individual Sub-processor:

a) description of the Sub-processor, including its contact details, company form and geographical location;

b) the type of service being provided by the Sub-processor;

c) assurances given that requirements in Applicable Data Protection Legislation will be complied with, and

d) where the Sub-processor is Processing the Personal Data covered by the DPA.

8.4 Should the Sub-processor fail to fulfill its obligations as regards the Processing of Personal Data according to the sub-processor agreement, Processor shall retain full responsibility in respect of Controller for the Sub-processor's obligations according to the Agreement and Applicable Data Protection Legislation.

9 Transfer to a Third Country

9.1 Processor may, either themselves or via a Sub-processor, Process Personal Data in a third country. If Processor is to Process Personal Data in a third country, prior to this Processor shall:

a) investigate whether such third country provides an adequate level of protection for personal data according to a decision announced by the EU Commission and if this is the case, Personal Data may be transferred to such third country, and if no such decision exists,

b) ensure that there are appropriate protection measures in place in accordance with Applicable Data Protection Legislation, e.g. standard contractual clauses adopted by the EU Commission or binding corporate rules that extend to the Processing of Personal Data.

10 Transfer to a Third Country

10.1 Controller, or a third party on its behalf, is entitled to access facilities, information and registers for the purposes of verifying that Processor and any Sub-processors are fulfilling the obligations set out in the Agreement. Processor undertakes to provide assistance to Controller to the extent required to enable Controller to gain assurance of this as simply as possible. If such effort requested from Processor is significant, Processor shall have the right to invoice Controller for such effort on a time and material basis, provided Controller has been notified thereabout before Processor commencing such chargeable work.

10.2 Processor shall allow the inspections required by the competent supervisory authority under Applicable Data Protection Legislation to gain assurance that Personal Data is being Processed in the correct manner. Processor shall comply with any decisions made by the competent supervisory authority regarding action required in order to satisfy Applicable Data Protection Legislation.

11 Termination of Processing

11.1 Following the termination of the DPA, Processor shall submit Personal Data to Controller if requested by Controller in accordance with the Agreement. Once Processor has submitted such Personal Data to Controller, or a request is not made in accordance with the Agreement, Processor shall delete the Personal Data in accordance with the Agreement in such a way that it cannot be recreated, unless storage of the Personal Data is required by law.

12 Remuneration

12.1 Besides what is stated in the Agreement or this DPA, Processor is not entitled to special remuneration to fulfill obligations according to the DPA or Applicable Data Protection Legislation.

13 Liability for Damage

13.1 In the event a Party is held liable for damages suffered by a data subject that have resulted from Processing Personal Data under the Agreement, the Party shall be entitled to, without limitation, claim back from the other Party that part of the compensation corresponding to the other Party's part of responsibility for the damage in accordance with Applicable Data Protection Legislation. Each Party shall compensate the other Party for reasonable and proportional costs of legal feels and proceedings arising from data subject claims. Processor's total liability under the DPA according to this clause 13.1 shall be limited to the limitation of liability amount set out in the Agreement.

13.2 In no event shall a Party compensate the other Party for administrative fines that have been imposed on the other Party.

13.3 Each Party's liability for types of damages other than those covered under this clause 13 is subject to the liability caps in the Agreement.

14 Changes to the Agreement

14.1 The terms of this DPA may be changed in accordance with the process for changes of terms in the Agreement.

14.2 This clause 14 does not prevent Controller from changing or issuing further instructions in accordance with what is set out in the DPA.

15 Term of Agreement

15.1 The DPA shall enter into force when the Parties have entered into the Agreement and shall thereafter remain valid until Processor ceases to Process Personal Data on Controller's behalf.

16 Governing and Disputes

16.1 The DPA shall enter into force when the Parties have entered into the Agreement and shall thereafter remain valid until Processor ceases to Process Personal Data on Controller's behalf. This DPA shall be governed by the substantive law of Sweden.

16.2 Disputes arising as a result of the DPA shall be settled according to the terms of the Agreement.

Appendix 1 – Instructions

This Appendix 1 of the Agreement describes the Processing of Personal Data that Processor will carry out on behalf of Controller under the Agreement.

a) Subject-Matter of the Processing

The subject-matter of the Processing is the Personal Data that Processor Processes on behalf of Controller in connection with the execution of the Agreement.

b) Type of Processing

The Processer Processes Personal Data in connection with the provision of a cloud-based digital asset management service for managing image, video, audio or other digital files. When Controller uses the service's web interface for Processing Personal Data, such use shall be treated as documented instructions for the Processing of Personal Data from Controller to Processor. Processor may Processes Personal Data manually, partly automated and/or fully automated. The Processing steps carried out by Processor on behalf of Controller is set-out in the table below and follow from what is otherwise stated in the Agreement.

Processing Operation	Description
Collection	Controller submits Personal Data to Processor by using a web interface that is provided by Processor. Processor's Product collects logs of Controllers usage of the web interface.
Transfer	Personal Data is transferred to/from Processors it-systems/Product.
Storage	Personal Data is stored on Processors it-systems/Product.
Updates, changes and deletion	Controller may update, change and delete Personal Data by using the functionality provided by the web interface and/or Product. Processor deletes Personal Data upon Controllers documented instructions.
Analysis	Processor analyses Personal Data to maintain the security of the web interface, the service and its it-systems; providing technical support; investigating misuse and abuse; and providing the functionality included in the service.
Sharing	Controller can access Personal Data and analysis reports via the service's web interface. Personal Data is shared with third parties via application programming interfaces and integration according to Controllers specifications. Otherwise, Personal Data is not shared without Controllers documented instructions.
Anonymization and Aggregation	Processor anonymizes Personal Data, logs and analysis reports. Such data may be used to create aggregated information, conclusions, and indices. All of the aforementioned output is anonymized and do not contain Personal Data.
Administration	Processor Processes Personal Data to provide Controllers staff with access to the service.
Data Export	Upon the termination of the Agreement and upon Controller's request, Processor exports Personal Data to Controller in accordance with the terms set out in the DPA and the Agreement.

c) Purpose of the Processing

Processor Processes Personal Data for the purpose of fulfilling its obligations according to the Service Agreement.

d) Type of Personal Data

The Processing may include:

- Name
- Logs
- Contact details
- Log-in details
- Images, video, and related metadata
- System Access
- Authorization Data
- Network identifiers
- Other types of personal data that Controller chooses to process in the service

e) Categories of Data Subjects

The Processing may cover:

- Controller's customers
- Controller's staff
- Controller's members
- Controller's suppliers
- Third parties

f) Physical Location of the Processing

The Processing will be carried out on equipment that is physically located in the EU/EES.

g) Duration of the Processing

The Processing will continue for as long as is necessary to provide and supply the services to Controller and fulfill obligations according to the Agreement.

h) Approved Sub-processors

The following Sub-processors have been employed with the written approval of Controller:

Name	Corp. reg. no	Type of processing	Geographical location
Iver Sverige AB	*556575-3042*	*Data hosting and operation partner*	*Stockholm, Sweden*
Google Cloud EMEA Ltd.	*IE660412*	*Cloud Based Data hosting and processing, infrastructure provider*	*Finland, Belgium, Netherlands*
Amazon Web Services EMEA SARL	*B186284*	*Cloud Based Data hosting and processing, infrastructure provider*	*Sweden and Europe*

Appendix 2 – Security instructions

This Appendix 2 of the Agreement contains instructions for Processor and an account of the technical and organizational security measures that Processor shall take in accordance with Section 4 of the Agreement.

a) Physical Security

IT equipment shall be protected against power failures and other disruptions caused in technical supply systems. Areas where Personal Data is stored or processed in some other way (e.g. server rooms and offices) shall be protected by appropriate access controls to ensure that only authorized personnel have access. It shall be possible to confirm the identities of all employees and visitors. IT systems and storage media shall be protected against damage and theft.

b) Computers and Mobile Devices

Processing of Personal Data on mobile devices shall be limited in accordance with documented procedures. The storage memories of mobile devices should always be protected with encryption.

c) Authentication

Logging into systems shall be carried out via personal user identification using a password and MFA (Multi Factor Authentication). Passwords shall be sufficiently strong and regularly changed. It shall not be permitted to assign or share login details to or with other individuals.

d) Authorization Control

Employees' access to Personal Data shall be controlled by a technical system for authorization control. Employees shall be granted the lowest possible level of access when processing Personal Data. Only employees who require access to Personal Data for their work shall be granted access.

e) Access Control

It shall be possible to verify access to Personal Data retrospectively via logs. Completed checks shall be documented and reported to Controller on request.

f) Servers

Access to administrative tools and interfaces on servers shall be restricted. Employees with administrative rights shall use strong passwords and MFA. It shall not be permitted to assign or share login details to or with other individuals. Documented procedures shall be in place to ensure that important updates to operating systems and applications are installed immediately.

g) Network Security

Networks shall be protected against external attack and loss of information. Wireless networks shall be protected using encryption. In- and outgoing network traffic shall be filtered, for example via firewalls. Software that regularly scans networks for malware (e.g. viruses, trojans, spyware and ransomware) shall be used and kept up-to-date.

h) Protection Against Malicious Codes

There shall be documented procedures in place to protect systems from viruses, trojans and other forms of digital infringement.

i) Backup

Personal Data shall be backed up regularly as set out in the Agreement. Backups shall be stored separately and well protected, so that Personal Data can be restored following a disruption.

j) Electronic Transmission

Connections for external electronic transmission shall be protected with technical functions that ensure the connection is authorized. Personal Data that is electronically transmitted outside the premises that is supervised by Processor (e.g. internet) shall be protected with encryption.

k) Destruction

There shall be possible to ensure that Personal Data can be irrevocably deleted once it is no longer required for the purpose.

l) Repairs and Servicing

When repairs and servicing of computer equipment are carried out by anyone other than Processor, a contract regulating security and confidentiality shall be entered into with the servicing company. Any servicing visits shall be carried out under the supervision of Processor. If this is not possible, storage media containing Personal Data shall be removed.

Servicing via remote data communication may only take place following secure electronic identification of the person carrying out the service. Servicing personnel may only be granted access to the system during the servicing visit. If there is separate communication access for servicing purposes, then this shall be closed when servicing is not being carried out.

m) Personal Data Breaches

Processor shall inform Controller promptly in the event of suspicion that a personal data breach has occurred, or when an actual breach has occurred. Processor shall be capable of restoring availability and access to Personal Data within a reasonable period of time following a physical or technical breach.

n) Personnel Training

Employees shall receive appropriate training in data protection before they are granted access to Personal Data.

o) Storage and Encryption of Personal Data with Cloud Based Sub-Processors

To the extent Processor utilizes cloud based sub-processors any stored Personal Data (at rest) with such cloud based sub-processor shall be physically located within EU/ESS and encrypted. The purpose of encryption is to improve the protection of Personal Data that is stored on a disk.

Encryption keys for such encrypted and stored Personal Data shall be stored outside of such cloud sub-processors and handled by an External Key Manager (EKM) within EU/EES.