Annex 1: Data Processing DPA (“DPA”)

1. Preamble

1.1. This DPA is an annex to the Parties concluded reference agreement the “Bitlog Online Service and License Terms and Conditions” (hereinafter ”Main Agreement”) for the provision of certain services, whereas the Service Provider is the Processor and the Customer is the “Controller”. Terms not defined in this DPA shall have the meaning as defined in the Main Agreement.

1.2. Processor processes personal data on behalf of the Controller to fulfill the Main Agreement. Controller determines the purpose and means of data processing. The Controller itself can be a processor and its principal is then the main controller. In that case, Controller’s principal determines the purpose and means of data processing.

2. Subject matter of this DPA

2.1. This DPA governs the collection, processing, and use of personal data (together “Processing” and “Process”) by Processor.

2.2. The services to be provided (“Services”) are described in the Main Agreement and summarized in Appendix 1 (Instructions for the processing of data) for the purpose of documentation and effective privacy monitoring.

2.3. According to this DPA, Controller or, if applicable, Controller’s principal, shall remain responsible for processing as controller. Processor shall be the processor.

3. Type and purpose of the processing

3.1. The type and purpose of the intended processing is set forth in Appendix 1 (Instructions for the processing of data) of this DPA.

4. Technical and organizational measures

4.1. Before the start of the processing, Processor shall implement such technical and organizational measures (“TOMs”) for the protection of Controller data which comply with the legally applicable requirements. The TOMs implemented within the scope of the DPA ensure the confidentiality, integrity, availability and resilience of the systems and Services in the long run in connection with the processing of Controller data. Processor shall document in writing the implementation of the TOMs and shall provide Controller with corresponding proof before the start of the Processing. If the verification sufficiently proves implementation of the TOMs, Controller will accept the proofs, and they will become an integral part of this DPA. If the verification is insufficient or the TOMs are not sufficiently implemented and Processor refuses to remediate the implementation, then Controller has the right to terminate the DPA for cause without notice.

4.2. Controller has the right and is obligated to adapt the TOMs to technical or organizational developments; in so doing, the level of protection may not fall short of the level of the agreed-upon TOMs. Substantial changes to the TOMs must be indicated by Processor and require a written DPA between the Parties. If implementation of necessary measures is not immediately possible, Processor shall take preliminary measures that sufficiently protect Controller data.

4.3. Controller has the right to suspend the Main Agreement for the period during which the level of protection is not sufficient as defined above. During the suspension of the Main Agreement, Processor does not have the right to demand the agreed payment or reimbursement for damages and expenses.

5. Rectification, restriction and erasure of Controller data; data portability

5.1. Processor is obligated to rectify, restrict or erase Controller data only after being instructed to do so by Controller.

5.2. Processor shall store Controller Data in a structured, commonly used and machine-readable format.

6. Processor's obligations

6.1. Processor may Process Controller data only within the scope of this DPA, for the agreed-upon purpose, with the agreed-upon means and according to Controller's instruction, unless Processor is obligated to different processing according to applicable national or EU law. Processor shall inform Controller of such an obligation before starting the activities according to this DPA. (i) Processing Controller Data for other purposes, (ii) duplicating Controller data, except for backups if they are an integral part of the services or are necessary to ensure proper Processing, or (iii) transfer of Controller data to third parties except and to the extent as expressively stipulated by this DPA or approved prior in writing by the Controller, is prohibited. This restriction also applies if the Controller data is anonymized or pseudonymized.

6.2. Processor shall process and store Controller data separately from its own personal data and that of other principals and shall sufficiently protect Controller data from being accessed by third parties.

6.3. Processor shall at Controllers request verify and ensure that it and its Sub-processors comply with the provisions in this DPA. Processor shall document its assessment in writing and shall make the corresponding documents available to Controller within six (6) weeks of Controller's requests

6.4. Processor shall fulfill its own documentation obligations according to data protection laws and keep that documentation up to date. Controller has the right to access and inspect that documentation. Upon request, Processor shall help Controller to create the Controller's own required documentation in accordance with data protection laws (e.g., records of processing activities). Processor shall provide Controller upon request with the necessary information for such documentation.

7. Location of Processing

7.1. The processing of Controller data by Processor or its Sub-processors shall take place at the locations listed in Appendix 1 (Instructions for the processing of data). Processor shall notify Controller before starting the processing if Processor is obliged under applicable law to process Controller data at another location, unless such a notice is legally forbidden. The Processing at and/or transfer to other locations during the term of this DPA must be documented and requires Controller's prior written consent if this processing and/or transfer takes place in a country outside of the EU/EEA or to an international organization. In this case, Processor is also obligated to ensure an adequate level of data protection, corresponding to the applicable legal requirements and their administrative and judicial interpretations at the location where the processing is carried out, or – at Controller's sole discretion – give Controller the option of ensuring an adequate level of data protection, inter alia, by concluding or acceding to EU standard contractual clauses.

7.2. Processor may only process Controller data outside of its or its Sub-processors operation facilities with Controllers prior written consent.

8. Confidentiality obligation and data protection officer

8.1. Processor shall bind all persons authorized to process Controller data to confidentiality unless they are already subject to an appropriate statutory obligation of confidentiality. The duty of confidentiality shall continue after termination or expiration of the DPA. Processor shall document this obligation and shall provide Controller with appropriate verification within six (6) weeks of Controller's request or within the scope of its audits according to Clause 11 of this DPA. Processor shall inform all persons authorized to Process Controller data of their obligations according to this DPA.

Processor shall – to the extent required by law – appoint a data protection officer, whom can carry out his or her activities according to legal provisions. Processor shall provide Controller upon request with the data protection officer's contact information for the purpose of direct communication.

9. Inquiries from data subjects and authorities

9.1. Processor shall immediately inform Controller of inquiries from data subjects and authorities as well as of any audit activities, measures, or investigations of an authority and to forward such inquiries to Controller if and to the extent they concern Controller data. Processor is not authorized to answer inquiries about this DPA from data subjects, authorities or other third parties without explicit instruction from Controller. Processor is obligated to support Controller comprehensively in providing information to authorities or other third parties and in fulfilling the rights of the data subjects in connection with the processing of Controller data.

9.2. If Processor is legally obligated to answer the inquiry of a competent authority itself or to comply immediately with an order itself, then Processor shall inform Controller of this without delay and in advance in order to enable Controller to prevent access to Controller data.

10. Engagement of Sub-processors

10.1. Processor has the right to engage other processors ("Sub-processors") for carrying out specific processing activities according to this DPA only with Controller's prior written consent. Employing Sub-processors to carry out substantial processing operations shall not be permitted unless this is explicitly an integral part of the Main Agreement. Controller already agrees to the Sub-processors listed in Appendix 2 (Authorized Sub-processors) of this DPA. Controller may not unreasonably refuse the use of Sub-processors if the requirements in Clause 4 of the DPA are fulfilled.

10.2. Processor shall formulate the DPA with Sub-processors so that it complies with the stipulations in this DPA, applies the same data protection obligations to Sub-processor as set out in this DPA and ensures the protection of Controller data in the same manner as this DPA. Clause 8 of this DPA (Location of Processing) shall apply correspondingly. In sub-contracting, Controller shall be granted the same supervision and audit rights regarding Sub-processor that are granted in this DPA. Sub-processor must agree to these obligations in writing. Upon conclusion of the DPA with Sub-processor, Processor shall upon request provide Controller with a copy of the legally signed sub-contract DPA, at least with the part of the DPA concerning Processing according to this DPA, including the agreed technical and organizational measures and/or proof of compliance with the TOMs and of the Sub-processor's reliability. Processor shall be liable to Controller for Sub-processor's compliance with the obligations.

10.3. Processor shall carry out audits at Sub-processor according to Clause 11 of this DPA.

10.4. Controller can demand at any time that a Sub-processor is replaced for cause or that Processor itself carries out the Processing. A cause is, not exclusively, a violation of Clause 4 of this DPA. If there is a cause and Processor cannot replace Sub-processor or carry out the work itself, then according to Clause 4, Controller has the right to terminate the DPA for cause.

10.5. Services that Processor sub-contracts to third parties as ancillary services to support Processor in providing the services under this DPA shall not be considered sub-contracting within the meaning of this Clause 10. In general, this includes telecommunications services, transportation services for mail and courier deliveries, security services and other services for which Processor is responsible for. In case of any doubt about the nature of a sub-contract as an ancillary service according to this clause, Processor shall agree upon with Controller about engaging this third party. However, even when sub-contracting ancillary services, Processor shall be obligated to ensure the protection and security of Controller data and other confidential information in connection with this DPA by entering into appropriate and lawful DPAs with the service providers and by adopting control and monitoring measures for sufficient protection of data and information.

11. Controller's audit rights and Processor's duties to cooperate

11.1. Controller shall be entitled, before the commencement of the Processing and, in its sole discretion regularly thereafter, to audit and inspect Processor's compliance with the terms and conditions of this DPA, in particular with regard to implementation of the TOMs stipulated in Clause 4 of this DPA. Controller has the right to carry out the audit itself or to assign the audit to third parties bound to confidentiality obligations. Processor may reject the assignment to specific third parties for cause. Controller shall endeavor not to interfere with Processor's normal business operations.

11.2. Processor shall grant Controller access for audit purposes to Processor's facilities or to all locations at or from which Controller data is processed during regular business hours. Controller shall notify Processor in writing of an on-site audit, if possible, two (2) weeks in advance. If Controller has reasonable suspicion that Processor is violating an applicable data privacy law or this DPA in a substantial manner, then Controller has the right to an on-site audit at any time without prior notice. If during an audit Controller finds any violations or irregularities, it shall grant Processor an appropriate period to remedy those violations or irregularities completely. Processor shall at its own cost take all necessary measures to remedy all violations or irregularities found.

11.3. Processor shall support Controller during the audits and grant Controller access to all documents, papers, and file records necessary for the audit as well as to allow Controller to inspect its systems to the extent they are used in connection with Processing of Controller data according to this DPA.

11.4. Processor may offer and provide substantive documentation to Controller to demonstrate and prove compliance with the provisions in this DPA and of the implementation of the TOMs. Such documentation can be in the form of a current attestation, of reports or report excerpts from independent bodies (e.g., accountant, auditor, data protection officer), an appropriate certification resulting from an IT security audit or from a data protection audit (e.g., according to ISO 27001), or a certification approved by the competent authority. Controller's right to carry out on-site audits remains unaffected; Controller shall decide in its sole discretion as to whether an on-site audit is necessary after submission of the documentation.

12. Authority to issue instructions

12.1. Processing of Controller data shall take place only within the scope of the provisions in this DPA and according to Controller's individual instructions. Processor shall only be bound to comply with Controller's instructions if they are given in writing or via email by Controller's representatives or appointed individuals for that purpose.

12.2. Within the scope of this DPA, Controller reserves the right to issue comprehensive instructions regarding the scope, type and method of the Processing, which Controller may specify by means of individual instructions. Any changes to the subject matter of the processing and the purpose of processing shall be subject to a mutual DPA in writing.

12.3. Processor shall immediately notify Controller if Processor reasonably believes that any of the Controller's instruction violates statutory provisions. Upon prior notification within reasonable time, Processor may suspend implementation and/or compliance with the relevant instruction, until its legitimacy is confirmed by the Controller in writing or until it is modified by the Controller accordingly.

13. Processor's reportable incidents

13.1. Processor shall inform Controller without undue delay but no later than 24 hours after having become aware of an incident or regarding a violation of security that, irrespective of being unintentional or unlawful, leads to destruction, loss, alteration, or unauthorized disclosure of or unauthorized access to Controller data that was transferred, stored, or Processed otherwise ("Incident"). Verbal notices shall immediately be confirmed in writing or via email. The written notice shall contain, in particular, a description of the nature of the Incident, including, when possible, the categories and approximate number of data subjects concerned, the categories and the approximate number of Controller Data and datasets concerned, and a description of the likely consequences of the Incident.

13.2. In the event of an Incident, Processor, in consultation with Controller, shall immediately take the necessary steps to secure Controller data and to reduce possible detrimental consequences for data subjects. Processor shall inform Controller regularly of developments and new findings and to make available to Controller within no more than five (5) days comprehensive documentation about the incident and its investigation, including, to the extent that it is appropriate and technically possible, a root cause analysis as well as information about the corrective measures taken.

13.3. If, in the event of an Incident, Controller or its principal is required to comply with statutory notification obligations to authorities and data subjects, Processor shall immediately support Controller to create the notification by providing documents and other appropriate proof, and by answering all of Controller's inquiries without undue delay. Processor shall reimburse Controller for all costs and expenses incurred in connection with the fulfillment of the notification requirements to authorities and data subjects if the notification requirement is due to a culpable breach by Processor or one of its Sub-Processor's according to Clause 10.

14. Liability and indemnity

14.1. The liability limitations agreed upon in the Main Agreement do not apply to liability from and in connection with this DPA or the processing of Controller data by Processor regardless of the legal basis of the liability claim.

14.2. Processor shall indemnify and hold Controller harmless from and against all demands and claims for damages that third parties, including data subjects, assert against Controller as a result of (i) Processor's breach of this DPA or of legal obligations, (ii) the Processor's failure to comply with instructions rightfully given by Controller, or (iii) an Incident for which the Processor is responsible. Processor shall indemnify Controller upon first demand. Processor shall reimburse Controller for all suitable defense and attorney costs to the extent the necessary defensive measures and settlement negotiations must be reserved and remain reserved to Controller. In this case, Controller has a claim to an advance payment in the amount of the estimated defense costs.

15. Duration, term, and termination

15.1. This DPA shall come into effect once both Parties have signed it, or at a later date which both Parties have agreed to. The term shall be the same as that of the Main Agreement. However, the provisions in this DPA shall apply after the term of this DPA and of the Main Agreement as long as Processor has possession of the data that is covered by this DPA and as long as there are further obligations resulting from the provisions of this DPA that go beyond the term of the Main Agreement.

15.2. Termination of the Main Agreement shall also lead to termination of this DPA, with the exception stated in Clause 15.1.

15.2.1. Controller has the right to terminate the DPA for cause if:

a) Processor violates this DPA or statutory provisions and does not rectify the violation within thirty (30) days of receiving a written request from the Controller; or

b) Processor violates provisions stipulated in Clauses 6 to 13 in this DPA in a substantial matter.

15.3. Statutory rights to terminate for cause shall remain unaffected.

16. Rights regarding Controller data and Processor's obligations after termination of this DPA

16.1. All of Controller data storage devices and Controller data shall remain the property of Controller. Furthermore, Controller shall retain all rights to know-how, copyrights, other usage rights and other intellectual property rights to Controller data or other information entrusted to Processor within the scope of this DPA.

16.2. Upon termination or expiration of this DPA or any time upon Controller's request, Processor shall return to Controller all Controller data obtained from Controller or obtained otherwise in connection with provisions of the services under this DPA as well as data media, documents, processing or usage results prepared, and databases that are related to this DPA, or to delete them upon Controller's instruction in a technically secure and irreversible manner unless and to the extent of an obligation under applicable national or EU law to archive such Controller data. The record of deleting and/or destroying the data shall be presented to Controller upon request. Processor shall bear the costs incurred in connection the obligations under this Clause.

16.3. Documentation that serves the purpose of verifying Processing according to the Main Agreement and applicable law shall be archived by Processor after termination or expiration of the DPA according to the relevant statutory period of retention. To discharge himself, Processor may transfer entirely that documentation to Controller upon termination or expiration of the DPA.

17. Measures by third parties

17.1. If Controller's property, including all Controller data, is endangered by third-party measures, including but not limited to search and seizure, an attachment order, confiscation during bankruptcy, insolvency, or settlement proceedings, Processor shall inform Controller immediately.

17.2. Processor shall also inform the above-mentioned third parties that Controller has the sole rights of disposal and rights to ownership of the

Processed Controller data and those statutory provisions that restrict the handling of this data.

18. Severability clause and form

18.1. If and to the extent that a provision of this DPA is unlawful, void, unenforceable or incompatible with the opinions of competent national or European authorities, that provision shall not affect the validity of the remaining provisions of the DPA. The Parties agree that such an invalid provision shall be replaced by a valid one that corresponds most with the Parties' original purpose regarding this DPA.

18.2. Amendments or supplement to this DPA must be made in writing. The same applies to amending or cancelling the written form requirement.

18.3. In the event of inconsistencies between this DPA and the Main Agreement or another DPA, the provisions of this DPA shall take precedence.

19. Signatures

Controller

____

[Name, title]
[Date, place]

Processor

____

[Name, title]
[Date, place]

Appendix 1 – Instructions for the processing of data

This Appendix is an integrated part of the DPA and constitutes the instructions from the Controller to the Processor in the course of the Processor processing personal data on behalf of the Controller.

By signing this DPA the Processor has confirmed the instructions stated in this Appendix 1. Amendments or supplement to this Appendix 1 must be made in writing. The same applies to amending or cancelling the written form requirement.

<u>The purpose of processing personal data by the Processor</u>

a. In order for the Processor to fulfill its obligations according to the Main Agreement as well as this DPA.

b. In order for the Processors to fulfill its obligations according to applicable data protections laws which are applicable to the Processor.

<u>Categories of personal data</u>

The categories of personal data which will be processed by the Processor:

a. Identification data: first name, surname, personal identification number and title of the Controller's contact person, employees, consultants as well as the Controller's customers.
b. Contact details: address, e-mail address, telephone number of the Controller's contact person as well as the Controller's customers.
c. Location data: IP address of the Controller's contact person as well as the Controller's customers.

<u>Place of processing</u>
The Processor shall process the personal data within the EU.

<u>Time Limit for data processing</u>
The Processor will process the personal data under this DPA for the term of the Main Agreement and for one (1) month thereafter if applicable data protections laws do not statue otherwise or the Processor is instructed otherwise by the Controller.

Appendix 2 – List of approved Sub-processors

1. Microsoft Azure

Place for processing: EU

The purpose of the processing of personal data: provide a cloud platform for the Services.