Terms on Processing of Personal Data

1. SUBJECT MATTER

1.1 These terms on the Processing of Personal Data ("**Terms**") apply to all processing of personal data by Syndis ehf., company number 580113-0600, Borgartun 37, 105 Reykjavik ("**Processor**" or "**Syndis**") where Syndis acts as a data processor when providing Customer ("**Controller**") Service. A description of the processing activities undertaken by Syndis can be found in a Master Service Agreement entered into between the parties (the "**Data Processing Description**").

1.2 All reference to the "**Data Protection Act**" shall in these Terms mean the Act on Data Protection and the Processing of Personal Data No. 90/2018 and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data on the free movement of such data, which entered into force on 25 May 2018 ("**GDPR**").

1.3 The terms "**controller**", "**personal data**", "**data subject**", "**processing**", "**processor**" and "**personal data breach**" shall have the meaning ascribed to them in the Data Protection Act.

1.4 These Terms apply to the Processor's processing of personal data which is necessary to provide the Controller the requested Services. If the parties have entered into a special processing agreement prior to these Terms entering into force, that agreement remains in force, unless otherwise agreed.

1.5 Any references to these Terms in a Master Service agreement entered into between the parties, or in an offer made by Syndis which is accepted by the Controller, as applicable, shall include acceptance of the Terms.

2. PARTIES' OBLIGATIONS

2.1 The Controller is fully responsible for fulfilling its legal obligation under the Data Protection Act, including providing adequate information to data subjects and making sure that all processing is lawful. The Controller shall also ensure that it is authorized to entrust the Processor with the processing of personal data and the Controller is solely responsible for the processing instructions provided to the Processor.

2.2 The Processor shall only process personal data to the extent necessary to provide the Controller the specified Services and in accordance with the Controller's written instructions. The Processor shall not process the personal data for any other purpose or in a way that does not comply with these Terms or the Data Protection Act. The Processor must promptly notify the Controller if, in its opinion, the Controller's instructions do not comply with the Data Protection Act and in such incidents the Processor is not obliged to follow the Controller's instructions.

2.3 The Processor shall maintain the confidentiality of all personal data and it shall not disclose personal data to third parties unless in accordance with these Terms, where such authorization is provided for in an agreement between the parties, the Controller provides special permission for dissemination of information or the Processor is legally obliged to do so.

2.4 The Processor will ensure that its employees:

(a) are informed of the confidential nature of the personal data processed and that they are contractually bound by an obligation of confidentiality,

(b) are aware of their confidentiality obligations imposed by legislation, including the Act on Financial Undertakings, as applicable,

(c) have undertaken training on the Data Protection Act relating to the processing of personal data;

(d) are aware of the Processor's obligations under the Data Protection Act and these Terms.

3. SECURITY OF PERSONAL DATA

3.1 The Processor shall implement appropriate technical and organizational measures, appropriate to the risk, to ensure level of security and to minimize the risk of unlawful or unauthorized processing of personal data. The measures shall seek to, as appropriate:

(a) ensure ongoing confidentiality, contiguity, and availability of personal data,

(b) ensure a process for testing and evaluating the effectiveness of measures safeguarding the processing, and

(c) ensure that adequate security measures are taken, having regards to the nature of the personal data processed, e.g. in terms of access control, the use of pseudo-identity and encryption.

3.2 The Processor is ISO 27001:2013 certified and has implemented security measures in accordance with the standard.

3.3 In the incident a Controller deems it necessary to implement extra security measures, in addition the measures the Processor has implemented in relation to specific Services, the parties shall enter into specific agreement in relation to such additional Service.

4. PERSONAL DATA BREACH

4.1 The Processor shall, without undue delay, notify the Controller after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed ("**Personal Data Breach**").

4.2 The Processor's notification shall include all information referred to in Article 33(3) of the GDPR.

4.3 The parties agree that the Controller is solely responsible for and has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any data subjects, supervisory authorities, or others; and

(b) how such notices shall be sent.

5. SUBPROCESSORS

5.1 If the Processor appoints a third-party subcontractor to provide the Services, or parts of it, and that requires the subcontractor's processing of personal data, the subcontractor shall be considered as **Sub-Processor** in the meaning of the Data Protection Act.

5.2 The Processor may only authorize a Sub-Processor to process personal data if the Processor has entered into a written agreement with the Sub-Processor that contains terms substantially the same as those set out in these Terms, in particular, in relation to the security of personal data.

5.3 Where the Sub-Processor fails to fulfil its obligations under such a written agreement, the Processor remains fully liable to the Controller.

5.4 The Sub-Processors used, in relation to each Service provided by the Processor, are listed in the Data Processing Description. By accepting these Terms, the Controller agrees to the Processor's use of the listed Sub-Processors.

5.5 If the Processor appoints a new Sub-Processor, it shall inform the Controller thereof and provide the Controller 14 days to object to such an appointment.

6. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

6.1 The Processor must not transfer personal data outside the European Economic Area ("**EEA**") unless the provisions of Chapter V of the GDPR are complied with.

6.2 Where the Processor transfers personal data outside the EEA, in relation to certain Services, information on such transfer shall be listed in the Data Processing Description. By consenting to these Terms, the Controller accepts such transfer. Additional transfer of personal data outside the EEA shall not take place unless the Controller is notified of such transfer and is provided with the opportunity to object to it, in accordance with Article 5.5 of these Terms.

7. DATA SUBJECT REQUESTS

7.1 The Processor shall assist the Controller, to the extent reasonable taking into consideration the nature of the processing, in responding to data subject requests. All work carried out by the Processor in relation to such assistance shall be subject to the parties' Agreement and/or the Processor's price list at any giving time.

7.2 The responsibility for responding to requests from data subjects shall always remain with the Controller.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1 Upon prior written request of the Controller, the Processor shall assist the Controller to carry out data protection impact assessment (DPIA) and in conducting prior consultation with the Icelandic Data Protection Authority. Such assistance shall however always take into account the nature of processing and the information available to the Processor.

8.2 All assistance with DPIA or prior consultation shall be subject to Service fees in accordance with the Processor's price list at any given time.

9. AUDIT

9.1 At least once a year, the Processor shall conduct an audit to evaluate its compliance with these Terms. This includes obtaining an external audit of its ISO 27001 certification performed by a recognized certification body.

9.2 The Processor undertakes to promptly address any exceptions noted in audit reports and implement necessary improvements.

9.3 The Processor shall furthermore make all information available to the Controller that are necessary to demonstrate compliance with these Terms, and to the extent possible taking into consideration the nature of the Service, allow for and contribute to audits by the Controller, or an auditor mandated by the Controller, for the purpose of verifying the Processor's compliance with these Terms. The audits shall only relate to the Services carried out by the Processor on behalf of the Controller and the scope of the audits shall take into account the Processor's obligations, such as in relation to security. Auditors and scope of audits are thus subject to the Processor's consent.

9.4 The Processor shall furthermore, in accordance with legal obligations thereof, ensure regulators' access to the personal data processed by the Processor on behalf of Controllers which are classified as regulated entities.

9.5 All assistance in relation to audits shall be subject to Service fees in accordance with the Processor's price list at any given time.

10. DURATION, DATA RETURN AND DELETION

10.1 These Terms shall remain in full force and effect until the termination of the Agreement.

10.2 Upon termination of Service, the Processor shall, at the choice of the Controller, delete or return all personal data to the Controller and delete existing copies. If the return of data calls for substantive work on behalf of the Processor, such work shall be subject to Service fee in accordance with the Processor's price list at any given time.

11. NOTIFICATIONS TO THE CONTROLLER

11.1 Notifications to the Controller based on these Terms shall be sent to the Controller's registered contact person. The Controller is responsible for providing the Processor with contact details of such a person. If contact persons are listed in the parties' Agreement, a notification shall be sent to that contact person, unless parties have agreed otherwise.

11.2 The Controller is responsible for providing the Processor with updated contact details.

11.3 The Processor can also publish all notifications, subject to these Terms, on its websites, on the condition that the Controller's contact persons

shall be informed of such notifications and have the opportunity to register for such notifications.

12. MISCELLANEOUS

12.1 The parties' Agreement and Syndis's General Terms shall, in addition to these Terms, apply to the Processor's processing of personal data on behalf of the Controller, including provisions regarding limitation of liability. In the event of any inconsistency between the provisions of these Terms and the provisions of Syndis's General Terms or the parties' Agreement, the provisions of these Terms shall prevail.

12.2 These Terms are governed by the laws of Iceland. Any disputes arising from or in connection with these Terms shall be brought exclusively before the District Court of Reykjavík.

12.3 The Processor reserves the right to amend these Terms in accordance with changes in relevant law or regulations or due to changes in how personal data is processed. The Processor shall inform the Controller of any changes made to these Terms. If changes, made to these Terms, materially affect the rights and obligations of the Controller, such changes shall not take effect until after a predetermined time, and if the Controller does not accept such changes after a notification is sent to the Controller, the Controller shall have the right to terminate the appropriate Service.