Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)
(as based on Opinion 14/2019 by the European Data Protection Board).

This Data Protection Agreement ("DPA") is part of the Whereby Terms of Service available at https://whereby.com/information/tos/, between Customer and Whereby, or other agreement entered into between Customer and Whereby governing Customer's use of the services provided by Whereby (the "Agreement") when Whereby is processing personal data on behalf of the customer. The DPA have been entered into in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject between the customer("the data controller") and Whereby AS with business address Gate 1, no. 107, 6700 Maaloy, Norway ("Whereby" or "the data processor").

1 Preamble

1. This Data Protection Agreement (DPA) sets out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The DPA have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 (General Data Protection Regulation).

3. In the context of the provision of the services to be provided under agreement entered into by the data controller and the data processor as described in Appendix A hereto, the data processor will process personal data on behalf of the data controller in accordance with the DPA.

4. The DPA shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the DPA and form an integral part of the DPA.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D may contain provisions for other agreements among the parties relating to data protection. In case of any inconsistency between the agreement and appendix D, the content of appendix D shall prevail, as long as the agreements in Appendix D do not contradict the

requirements set in Article 28 GDPR.

10. The DPA along with appendices shall be retained in writing, including electronically, by both parties.

11. The DPA shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2 The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the DPA.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other things, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3 The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the data processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the DPA.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4 Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5 Security of processing

[1] References to "Member States" made throughout the DPA shall be understood as references to "EEA Member States".

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;
   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix D.

6 Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of The DPA without the prior general written authorisation of the data controller.
   a. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least four weeks in advance, thereby giving the data controller the opportunity to object to such changes and terminate the agreement with the data processor prior to the engagement of the concerned sub-processor(s), provided that the controller has substantial and documented reasons for such objection. The list of

sub-processors already processing the data can be found in Appendix B.

3. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the DPA and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the DPA and the GDPR.

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the DPA are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

5. The data processor shall agree to a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7 Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the DPA:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization
   b. transfer the processing of personal data to a sub-processor in a third country
   c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country

including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The DPA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the DPA cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8 Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 5.3, the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Norwegian Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, the Norwegian Data Protection Authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

9 Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 8 2. a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix D all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10 Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

11 Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the DPA and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to

applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12 The parties' agreement on other terms

1. The parties may in agree in Appendix D on other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the DPA or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13 Commencement and termination

1. The DPA shall become effective on the date of the creation of the Data Controller's account in Whereby.

2. Both parties shall be entitled to require the DPA renegotiated if changes to the law or inexpediency of the DPA should give rise to such renegotiation.

3. The DPA shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, The DPA cannot be terminated unless other DPA governing the provision of personal data processing services have been agreed upon between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the DPA may be terminated by written notice by either party.

14 Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points: admin users in the account of Data Controller will act as contact points. The Data Processor may assign an account manager or other point of contact, and can be contacted regarding this agreement on legal@whereby.com

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Appendix A - Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data

controller is:

To enable the data controller to exercise account management including room ownership allocation and configuration for the service provided as described in agreement entered into by the data processor as supplier and the data controller as customer.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The processing of personal data which the data processor does on behalf of the controller consists in making Whereby's web-based video communications services and related supplementary services available for the users of the controller, by enabling the controller to manage the account including room ownership allocation and configuration.

The parties acknowledge that the data processor will be controller for other processing activities as described in the Privacy Policy and Terms of Service of the data processor, including transmission of the communication, fault and error detection and handling, security, developing the service, provision of customer support, billing, user activation and engagement, marketing and sales activities of the data processor.

The parties also acknowledge that the participants to a video conferencing call (or the legal persons they represent) will be the sole controllers of their disclosure of content within a call, and recipients(or the legal persons they represent) will be the controller for their use of content received in a call.

For information where the data processor is the data controller, Whereby Terms of Service and Privacy Policy applies.

A.3. Processing includes the following category of data subject:

• Persons who have personal user accounts for authentication / login to the service ("users").

A.4. The processing includes the following types of personal data about data subjects:

Persons who have personal user accounts for authentication / login to the service ("users").

Users are persons who have a registered account in the service on the web (a "user account"). Typically, these persons will manage the setup of their room(s), they can also be "admin" or for an organization with many users (a "Business account").

The following information about these data subjects are processed:

• Display Name
• Email address
• Admin user (yes / no)
• Date / timestamp for creation / updating / activating the user account
• Organization affiliation - for personal user accounts associated with a Business account
• Video rooms created
• Room name
• Profile picture
• Background picture
• For users that opt to use Google as a third-party authentication mechanism for logging in to Whereby, the following additional information is processed:

- Google account userID
- Display name
- Profile image URL

Note on usage information: In order to develop the product in accordance with users' needs and ensure safe and non-abusive usage, the technical performance and security of the product, as well as being able to bill customers correctly based on their usage, the data processor needs to track certain usage information about users' navigation in the product. As the data processor determines the scope and purpose of this usage information, it is the data processor who will be the data controller for this information. The individual user will be the data subject, the processing of this information will be governed by Whereby Privacy Policy and the user will retain all their rights under GDPR.

Note on call data (audio, video, screen sharing, chat and other content): Whereby operates a global infrastructure of video routers distributed across the world, and users will be automatically routed to the closest available one to them. IP addresses will only be used to connect the user with a data center in their region. This means that e.g. users in European countries, will connect to a data center physically located within the EEC. The video router servers and all of Whereby's infrastructure adhere to strict security measures, preventing any eavesdropping or interruption of the video/audio streams. Media sent between participants in a room will not be stored. Hosting providers used to route video calls do not have ability to access or control the data streams, nor is any transmission initiated by them, and data sent through Whereby is initiated by the customer, the customer select the receiver of the transmission and nor Whereby nor its subcontractors are able to select or modify the information contained in the transmission, cf. GDPR Article 2 (4). The data processor (Whereby) is the controller of transmission of call data, and the processing will be governed in the Whereby Privacy Policy, and the data subject will retain all their rights after GDPR.

Users can choose between "Small" room size (up to 4 participants) and larger rooms. In "Small" room size, communication between participants are primarily sent through peer-to-peer connections, where audio and video streams are sent directly between participants and do not pass through any of our servers, in cases where this is allowed by the network the user is on. Video and audio transmitted in the Service is then sent directly between the participants in a room and is encrypted (DTLS-SRTP) with client-generated encryption keys. In cases where a user is behind a strict firewall or NAT (e.g. on a strict corporate networks), video and audio need to be relayed via a TURN server, but end-to-end encryption is still maintained.

Calls using a larger room size will use a dedicated server infrastructure to allow more people in conversation, and better stability. The video stream will be sent through video router servers which transmits it to the other participants in the call, and also transmits their streams to the organizer. Streams will always be encrypted (DTLS-SRTP) in transit, but will be decrypted and re-encrypted when passing through the video routers.

The system is designed to comply with European privacy regulations (such as GDPR) and as long as it is recognized that the IP connecting to the TURN server is located in Europe, the user is guaranteed to connect to a server in the EEA. Data centers are dedicated for traffic in those regions and will only be used if a participant is located within one of those countries/regions. Data is always encrypted as it passes through the data processor's servers, the hosting providers used do not have the theoretical opportunity to intercept the traffic.

The "Recording" add-on which is available in the Pro and Business plans only allow client-side recording, so the recording is never uploaded to Whereby's servers. The user who starts the recording (the user must be a host in a room to do this) are then responsible for getting consents from all participants in the meeting prior to starting the recording. They are also responsible for

storing and processing the recording in compliance with regulations after downloading it from Whereby.

Chat messages are not stored permanently. They pass through Whereby's server that connects the users in the call temporarily in order to pass them on to each participant in the call, but are deleted from the server as soon as it has been delivered to the participant's computer. Additionally, as each participant leaves the room the chat messages that were stored locally on their computer are deleted. Controllers using the Meetings API will have the option to disable chat entirely.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the DPA commences. Processing has the following duration:

The processing shall be performed as long as the data processor provides the services under the Agreement to the controller, or the controller removes the relevant personal information from the service provided, or the personal information is removed by the data processor in accordance with the instructions detailed in this Appendix C.

Appendix B - Authorized sub-processors

C.1. Approved sub-processors

On commencement of The DPA, the data controller authorises the engagement of the following sub-processors:

NAME	COUNTRY	DESCRIPTION OF PROCESSING
Amazon Web Services EMEA SARL	Luxemburg, Ireland	Storage of User account information

The processor will communicate changes in the list to any users who are admins in the controller's account at that time, by email. At all times, an updated list of subprocessors can be found in the "Data Processing Agreement" section in the Terms of Service on Whereby's website.

Appendix C - Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the processing as described above in this DPA and as described in the Agreement.

C.2. Security of processing

The level of security shall take into account:

The services of the data processor are designed with the intention of minimizing the collection of personal information. The data required to use the service is limited to what is needed to authenticate a user and give them access to their own account, and data that is needed for the features in the services to work. There are no special categories of personal data stored, thus implying low risk in the case of a breach. But due to the volume of users in the service, a breach will impact many users. Special attention should be placed on audio and video content, which will be processed by the service in stream, but never stored.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

The data processor has designed the service and the routines of the data processor to have a high level of security and prevent any breaches. Testing is integrated in the development process, and a system for continuous deployment with automated tests running before deployment is in place. The infrastructure of the data processor has been designed to prevent any eavesdropping being possible on audio and video streams, with high levels of encryption.

The data processor has strict processes for requiring any personnel to sign NDAs or contracts containing confidentiality DPA before access is given to systems which contain data processed on behalf of controllers. Access is given on a need-to-know basis. The data processor has established a routine for offboarding of employees who leave.

The data processor has an appointed Data Protection Officer which is responsible for the routines related to privacy and security.

The data processor has a Data Protection Policy in place. This policy, along with risk assessment, routines and security objectives shall be reviewed regularly in order to ascertain whether it is appropriate in relation to the needs of Whereby, market conditions and threats.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 8.1. and 8.2. by implementing the following technical and organisational measures:

Individual users may download the information stored about them in the service through a self service function in their Profile Settings page (when they are logged into their account).

Individual users can delete their use profile entirely, also deleting any data stored about them with

the data processor.

Admin users in the controller's account may delete any user in the account, also deleting any data stored about them with the data processor.

Admin users in the controller's account can at any time see a list of all users in the account, and a list of all rooms created in the account.

C.4. Storage period/erasure procedures

Personal data is processed by the data processor on behalf of the controller for as long as the data processor provides the services to the controller under the Agreement after which the personal data is automatically erased by the data processor. If the data processor processes personal data as a controller, the personal data will be erased/anonymised according to the retention schedule set out in the Privacy Policy of the data processor.

Personal data that the data processor processes for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 10.1 (save for the retention as set forth above), unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the DPA.

C.5. Processing location

Processing of the personal data under the DPA cannot be performed at other locations than the following without the data controller's prior written authorisation:

The location for the processing is listed in Appendix B (approved sub-processors).

C.6. Instruction on the transfer of personal data to third countries

For subcontractors located outside the EEA, the transfer of personal data shall be done according to the regulation on transfers to third countries in Article 45 to 47 and 49 GDPR.

The data processor may transfer personal data to third countries if there is a legal basis for such transfer. The data processor will use the standard contractual clauses for transfer of personal data outside the EU/EEA provided an adequacy decision does not apply to the transfer. The data processor is hereby authorised to enter into the standard contractual clauses for the transfer of personal data to sub-processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council as notified under document C(2010) 593 ("the Standard Contractual Clauses for transfer to third countries") as decided under commission decision of 5 February 2010, or any updates to the standard contractual clauses decided by the Commission at a later date, on behalf of the controller with a sub-processor in a third country with the data processor as Data Exporter and the sub-processor as Data Importer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The data processor and the controller shall cover their own costs with regard to any audit. If the controller requests the use of an external auditor, the controller shall cover the costs on use of such auditor.

Appendix D Other terms of agreement among the parties.

None.