Jimber Network Isolation - Terms and Conditions

SERVICE PROVIDER

Jimber services are provided by, and you're contracting with:

Jimber BV, with registered offices at Patotterijstraat 76, 9250 Waasmunster, Belgium, registered in the CBE with number BE 0684.939.269, represented by one of its directors, Mr. Kristof Van Stappen,

Hereinafter referred to as: "**Jimber**",

And:
These terms help define the relationship between you and Jimber. Broadly speaking, we give you permission to use our services if you agree to follow these terms. You will be referred to as "the Customer".

TAKING INTO CONSIDERATION THAT:

- Jimber is an IT security provider who has developed several packages including IT- and cybersecurity services;
- The Customer, an organization, utilizes Services provided by Jimber.;

HEREBY AGREE ON THE FOLLOWING:

1. DEFINITIONS

1.1. **Agreement:** the present agreement and its annexes;

1.2. **Bug**: an error, defect or malfunction in a computer programme or system that causes it to produce an incorrect or unexpected result, or causes it to behave in an unintended manner;

1.3. **End User**: the person(s) working at the Customer who will use the Services;

1.4. **Services**: the software and/or services offered by Jimber;

1.5. **Territory:** worldwide;

2. PRICES AND PAYMENT

2.1. Prices for Jimber's services are available upon request through your designated reseller.

2.2. The Customer will receive invoices for the Services from their Reseller, unless otherwise agreed upon.

3. ORDERS

3.1. The customer can order the Services of Jimber in the application provided by Jimber.

3.2. Orders are automatically accepted when the Customer adds new End-Users, or a new Customers in the application provided by Jimber

3.3. Requests for NIACs (Network Interface Access Controllers), physical network controllers, and industrial network controllers can be made through the Customer's reseller.

3.4. NIACs (Network Interface Access Controllers), physical network controllers, and industrial network controllers remain the property of Jimber.

4. CHANGES TO THE SERVICES

4.1. Jimber has the right to make changes to the Services without prior notice. Jimber shall not be obliged to make these changes to the Services in the possession of or already ordered by the Customer.

4.2. Jimber will not remove any core functionality of the products without prior notice to the Customer. Core functionality refers to any feature or function that is essential to the proper functioning of the product as described in the product documentation. If Jimber determines that a core functionality must be removed, it will provide written notice to the Customer at least thirty (30) days prior to the removal of such core functionality.

4.3. Jimber has the right to stop the sale of one or more Services. Jimber shall give three (3) months' prior written notice of its intention to discontinue, if the Services are in the possession of or have already been ordered by the Customer.

4.4. The Customer cannot hold Jimber liable for changes referred to in article 4.1. The Customer has no recourse against Jimber on account of the fact that the latter no longer supplies the Services previously sold by Jimber, if the notice period referred to in article 4.2 was respected.

5. WARRANTIES

5.1. Jimber warrants to the Customer that the Services are fit for their intended use and comply with the mandatory standards applicable to the Services. Jimber does not provide the Customer with any other warranties in relation to the Services.

5.2. Jimber warrants that the software provided to the Customer shall function in accordance with the relevant documentation provided by Jimber.

5.3. Jimber will respect the integrity and confidentiality of the IT-infrastructure of the Customer. Jimber uses recognised and secure software according to the current state of the art. The

Customer accepts and acknowledges that Jimber's Services constitute a commitment of means ("*middelenverbintenis*") and not a result commitment. The Services provide a higher security protection of the IT-infrastructure of the Customer, however, can never completely rule out potential cyber attacks.

5.4. Each Party warrants and represents that:

i) it has full authority to enter into the Agreement and to perform the obligations required hereunder;

ii) the execution and performance of its obligations under the Agreement does not violate or conflict with the terms of any other agreement to which it is a Party and is in accordance with any applicable laws.

5.5. The Customer shall make no warranties on behalf of Jimber and will make no statements or representations that are inconsistent with those provided in this Agreement.

6. DURATION AND TERMINATION

6.1. The Agreement is concluded for a period of one (1) year starting on the date of confirmation of the Agreement.

6.2. After the first renewal of the Agreement, each Party has the right to terminate the Agreement at any time by providing one (1) months prior notice in writing.

6.3. Either Party is entitled to terminate the Agreement with immediate effect and without prior court intervention if the other Party commits a serious breach of its obligations under this Agreement and fails to correct or terminate such breach after receiving a written notice requesting the defaulting party to correct or terminate the breach within 30 days of receipt.

6.4. Jimber is entitled to terminate the Agreement with immediate effect and without prior court intervention if any of the following events occur:

i) if the Customer ceases payments, files for bankruptcy, is declared bankrupt or commences liquidation or similar proceedings;
ii) if control of the other Party changes hands.

6.5. Any notice or termination of this Agreement shall be done in writing by means of registered letter.

6.6. Upon termination of the agreement, all NIACs, physical network controllers, and industrial network controllers must be returned to the reseller or Jimber.

6.7. In the event that the customer fails to return the NIACs, physical network controllers, and industrial network controllers within a period of three months following the termination of the

agreement, Jimber will issue an invoice for the non-returned items. The invoiced amount will be calculated as follows: monthly rate per device multiplied by 24.

6.8. For items returned with customer-caused damage or defects, charges will also be 24 times the monthly rate per device.

7. LIABILITY

7.1. Jimber shall only be liable to the extent specified in the Service Level Agreement in Annex 1 as well as for damages resulting directly from an intentional fault or gross negligence committed by Jimber. The Services constitute a commitment of means ("*middelenverbintenis*") of Jimber.

7.2. Under no circumstances shall Jimber be held liable for any indirect or consequential damages, including, but not limited to, loss of savings, revenues or profits, or reputation damages.

7.3. The Customer shall be liable for and shall hold Jimber harmless against claims by any third party relating to the Services that are based on or originate in a violation by the Customer, through an act or omission, of any of its obligations under this Agreement.

7.4. Jimber cannot be held liable for any damages resulting from errors in the configuration executed by the Customer.

7.5. In any event, the liability of Jimber and the Customer will be limited to its insurance company's coverage. Jimber and the Customer have concluded an insurance policy that can be consulted by the other Party upon his written request.

8. DATA PROTECTION

8.1. Each Party shall at all times comply with its respective obligations under all applicable data protection legislation in respect of all personal data processed under the Agreement. To the extent that Jimber would process personal data for the benefit of the Customer in its capacity as processor, the Customer, in its capacity as controller, shall remain responsible for determining the purpose and manner of processing and Jimber shall comply with all instructions reasonably provided by the Customer in this regard.

8.2. Annex 3 contains a Data Processing Agreement by Jimber that can be provided by the Customer.

8.3. All questions of the Customer related to the Data Processing Agreement can be addressed via the e-mail address security@jimber.io .

9. FORCE MAJEURE

9.1. Neither Party shall be liable for any failure or delay in performing its obligations or for any loss, inconvenience or damage suffered by the other Party where such failure or delay is due to, or arises from, circumstances of a force majeure nature.

9.2. For the purposes of this Agreement, force majeure includes, but is not limited to, the following non-exhaustive events: natural disasters, fire, floods, strikes, pandemics, epidemics, labour disputes or industrial disturbances, embargoes, legal restrictions, governmental measures and industry-specific force majeure, such as internet disruption, electricity disturbances, the inaccessibility of the IT-systems due to cyber attacks.

9.3. The non-performance caused by an event qualified as force majeure must be notified in writing by the Party claiming force majeure to the other Party immediately and at the latest within 24 hours after the occurrence of the force majeure.

10. MISCELLANEOUS PROVISIONS

10.1. The Agreement contains the entire agreement between the Parties relating to the subject matter of the Agreement and supersedes all previous negotiations and agreements. Unless expressly provided otherwise in the Agreement, the Agreement may only be amended or modified by a written agreement signed by duly authorized representatives of both Parties.

10.2. If any part or clause of the Agreement is found to be invalid or unenforceable for any reason, the remaining parts or clauses shall not be affected thereby and shall remain valid and enforceable as if the invalid or unenforceable parts or clauses were not included in the Agreement.

Any such section or clause shall be replaced by the Parties with a provision which, so far as may be lawful, comes closest to what the Parties sought in the invalid or unenforceable section or clause.

10.3. The Parties agree that failure of either Party at any time to require performance by the other Party of any of the provisions herein shall not operate as a waiver of the right of that Party to request strict performance of the same or like provisions, or any other provisions hereof, at a later time.

11. APPLICABLE LAW AND COMPETENT JURISDICTION

11.1. The Agreement shall be governed and interpreted in accordance with Belgian law.

11.2. The applicability of the Vienna Convention is expressly excluded.

11.3. In the event of any dispute regarding the conclusion, performance, termination and/or interpretation of the Agreement, the Parties undertake to engage in good faith discussions with a view to resolving the dispute amicably.

11.4. If no resolution can be reached between the Parties after a reasonable period of time, the Parties shall try to settle such dispute in good faith through mediation. The parties will appoint an accredited mediator from the list of mediators of the CEPANI: www.cepani.be, before resorting to arbitration.

11.5. If the Parties do not reach a settlement through mediation, any unresolved dispute shall be settled by arbitration administered by the Body CEPANI: www.cepani.be, who will make a binding decision.

11.6. This article does not waive Jimber's rights based on the articles 1394/20 to 1394/27 and article 735, §2 of the Belgian Judicial Code regarding the collection of undisputed debts.

ANNEX 1 - SERVICE LEVEL AGREEMENT

1. OBJECT

1.1. This Service Level Agreement (hereinafter: "SLA") defines the additional terms and conditions for the Services regarding the support and maintenance provided by Jimber.

1.2. Jimber shall use all reasonable means to provide functioning Services. The Customer acknowledges and accepts that the Services increase the security of IT-systems, however, can never completely eliminate the risk of cyberattacks.

1.3. The Customer acknowledges and accepts that the compensations provided in this Annex cover the entire damage suffered and Jimber shall not owe any other compensation. The Customer also accepts that the estimate of the damage may be proportionally reduced if it is at least partly due to the Customer's failure to comply with its obligations set out in this Annex.

1.4. Are explicitly excluded from the scope of this SLA, damages resulting from:

a) errors in use of the Services;
b) incorrect or unauthorised use of the Services;
c) data integrity;
d) errors in software not provided by Jimber;
e) errors in hardware;
f) errors due to force majeure.

In these cases Jimber can help to try to solve the problem after all, but this support will be provided on a time-and-expense basis and will be invoiced at the applicable hourly rates.

2. CONTACT PERSONS

2.1. Jimber designates the reseller of the Customer as the primary contact person. For any inquiries or assistance, the reseller should be contacted.

3. OBLIGATIONS OF THE CUSTOMER

3.1. In order to enable Jimber to fulfill its obligations under this SLA, the Customer undertakes to:

a) always provide adequate access to the premises, systems, software, hardware and other infrastructure, whether physical or remote, to Jimber, its representatives and its employees, and grant the necessary permissions to do so;

b) to appoint competent persons as contact person for Jimber, in order to have contacts during support run as smoothly as possible, and in any case within the set response times;

c) report any problem that manifests itself immediately, correctly and completely to Jimber, in accordance with this Annex; and

d) make reasonable efforts to prevent (further) damage.

4. SECURITY AND CONFIDENTIALITY

4.1. When performing maintenance and support services, Jimber will always respect the confidentiality and integrity of the IT-systems of the Customer. Jimber will use recognised and market-compliant software to provide the maintenance and support.

5. DATA STORAGE AND BACKUP

5.1. Data is backuped on a daily basis to a cloud provider and stored on multiple locations. Data is backuped on a monthly basis on offline media stored in Jimber offices.

6. SECURITY

6.1. Our cloud service backend is protected by firewalls and advanced DDoS prevention measures to ensure the security of the system. In addition, all servers are secured with 2FA login and public-private key encryption to prevent unauthorized access. Access to our servers is only available from a select number of locations to further increase the security of the system.

7. MONITORING

7.1. Our cloud service backend is constantly monitored by a dedicated monitoring service that operates 24/7. In the event of any issues, the Jimber support line is automatically alerted.

8. MAINTENANCE

8.1. Jimber undertakes to provide maintenance to the Services from time to time. Such maintenance may be preventive or innovative in nature and may consist of updating the software by means of updates, solving known problems by means of patches or installing new versions.

9. AVAILABILITY

9.1. Scope

The provisions in this article 3 are only applicable if the Services are hosted on the infrastructure of Jimber (or its subprocessors). If the Reseller or the Customer itself provides the hosting or has it

provided by a party of its own choosing, and the Services are thus not hosted on infrastructure of Jimber (or its subprocessors), Jimber does not guarantee a service level regarding availability and Jimber cannot be held liable nor be obliged to pay compensation if the Services are unavailable.

9.2. Guarantee

Jimber guarantees that the Services will be available ninety-nine (99) percent of the time during the measurement period. The measurement period is one month.

9.3. Calculation

The availability will be calculated as follows:

Availability = (planned uptime - downtime) / planned uptime

In which:

a) Planned uptime: means the total number of minutes of availability during the measurement period.
b) Downtime: means the time that the Services are unavailable.

The following events are not taken into account to calculate availability:

a) Scheduled downtime: the time required to perform regular maintenance activities to maintain the Services;
b) Emergency maintenance: maintenance required to ensure the safety, performance or integrity of the Services due to a threat or vulnerability;
c) Force majeure;
d) Downtime resulting from a wrongful act, act or omission of the Customer or an End-User or a third party, except those that were foreseeable by Jimber or as a result of insufficient protection or security by Jimber;
e) Downtime resulting from a breach by the Customer or End-User of the Acceptable Use Guidelines in Annex 2.

9.4. Compensation

If the guarantee provided in art. 3.2 is not met, Jimber shall owe a fee of 10% of the monthly fee for the Services for every 1% below the agreed availability percentage.

The fee will be deducted from the next invoice. If there is no next invoice (e.g. due to the termination of the Agreement), Jimber shall issue a credit note and refund the fee.

10. FIRST AND SECOND LINE SUPPORT

The Resellers shall provide a helpdesk to the Customer providing first- and second-line support for

user queries, for logging, for tracking Bugs and for configuration settings.

11. THIRD LINE SUPPORT

11.1. General

Jimber shall provide a helpdesk providing third-line support. The third line support consists of code adjustments and server-specific problems. Only the Distributor and/or its Resellers may use the third line support offered by Jimber.

ANNEX 2 - ACCEPTABLE USE GUIDELINES

1. OBJECT

These Acceptable Use Guidelines set out the obligations and responsibilities of the Customer and End-User in connection with the use of the Services. The Customer and End-User must ensure and warrant that users are aware of these obligations and responsibilities and comply with them when using the Services.

2. AUTHORIZED USE

The Customer may only use the Services for its intended purpose and in combination with the equipment and materials necessary to enjoy the benefit of the Services.

Any instance of our server software that is installed on client-operated systems, including but not limited to local servers, virtual machines, or cloud environments, will be subject to additional licensing fees. These fees will be charged at the standard user rate per instance.

3. PROHIBITED USE

The Services may not be used for illegal or irresponsible acts. The following non-exhaustive list of activities shall in any case be considered to be illegal or irresponsible:

i) Using the Services to cause harm to minors (e.g. child pornography);

ii) Transmitting, distributing, publishing or displaying any material that

   a) endangers the safety or health of any person or may harm institutions, public safety or public health;

   b) is excessively violent or incites violence, threatens violence, has intimidating content or contains hate speech;

   c) promotes illegal drugs, violates export regulations or is related to illegal gambling activities or illegal arms trafficking;

   d) interferes with network systems and/or solution and/or network services or network communications; or

   e) infringes (via uploading or otherwise) the copyrights, patents, trade and/or other secrets or other (intellectual) property rights of third parties.

iii) Making fraudulent offers, buy or sell fraudulent goods or services or to promote scams;

iv) Collecting or using (personal) information without the consent of the owner of the information, for example e- mail addresses, screen names, e-ID cards, payment card and/or credit card details or other user identification, in order to exercise activities such as phishing, internet scamming, password theft, spidering or harvesting;

v) Intentionally spreading viruses or introducing other types of malicious programmes into the network or system aimed at damaging (or threatening to damage) the systems, software or data of third parties;

vi) Misusing the Services to access or attempt to access third-party accounts;

vii) Violating the integrity of computer and network systems, including developing or using programmes that obstruct other users or that infiltrate and/or damage a computer, computer system or network or that modify the software components of a computer, computer system or network;

viii) Obtaining or attempting to obtain access to the accounts of third parties, or infiltrate or attempt to infiltrate the security of the computer software or hardware, electronic communication systems of the Services or any third party.

4. SECURITY

To protect the Services, it is the responsibility of the Customer to ensure that:

i) access is granted only to users and that users have access only to their accounts;

ii) login data is protected and secured;

iii) the Services are only used in combination with the appropriate equipment;

iv) the equipment contains the necessary protection measures (e.g. anti-virus software, firewalls, etc.).

It is forbidden to:

i) circumvent the user identification or security of the Services, network or account or grant themselves or the users unauthorized access to data and/or grant themselves or the users access to data not intended for you or them;

ii) log into or use any server or account to which the Customer or the End Users do not have access;

iii) use tools designed to circumvent or break security measures or introduce or use tools designed to create excessive requests (e.g. (distributed) denial-of-service attacks) to crash the Services.

5. BREACH OF THIS ACCEPTABLE USE GUIDELINE

The Customer acknowledges and accepts that compliance with these Guidelines constitute an essential obligation of the Agreement. As such, Jimber has the right to remove the access of the Customer to the Services in case of violation or non-compliance with these Guidelines.

Without prejudice to any liability provisions, in the event that the Customer and its End Users violate these Guidelines, the Customer shall also defend, indemnify and hold Jimber harmless against any damages, losses, expenses, liabilities or claims that Jimber may incur as a result.

A breach of these Acceptable Use Guidelines may also result in criminal and/or civil prosecution.xr acknowledges and accepts that Jimber will cooperate with competent authorities and/or relevant third parties to investigate criminal and other undesirable activities related to the misuse/use of the Services.

ANNEX 3 - DATA PROCESSING AGREEMENT

Between:

Jimber bv, having its registered office at Patotterijstraat 76, 9250 Waasmunster and registered in the CBE under number BE 0684.939.269 represented by Kristof Van Stappen;

Hereinafter: "**the Processor**",

And:

You as a customer;

Hereinafter: "**the Customer**",

Hereinafter referred to collectively as "Parties" or each separately as "Party".

TAKING INTO CONSIDERATION:

- The Processor is a service provider in the cybersecurity sector;
- The Customer would like to rely on the Processor to carry out the processing activities of Schedule 1 to this Data Processing Agreement (hereinafter: "**DPA**") under the conditions stipulated in the Agreement;
- This Agreement is created within the framework of the obligation arising from Article 28 of the General Data Protection Regulation 2016/679 of 27 April 2016.

AGREE ON THE FOLLOWING:

1. Meaning of terms

All terms used in this DPA shall have the common meaning as defined in the Regulation or as derived, in order, from the case law of the European Court of Justice, the Market Court, the Belgian Data Protection Authority, other European data protection authorities and courts.

2. Object

2.1. The DPA regulates the rights and obligations of the Customer and the Processor when processing the Personal Data.

2.2. The Processor undertakes, as from the entry into force of the DPA, to comply with this DPA when carrying out processing activities on behalf of the Customer. If any processing

operations were already being carried out before the entry into force of this DPA, the Processor will in any event as from the entry into force of the DPA carry out such processing in accordance with the DPA.

3. Data Protection Officer (DPO)

3.1. All questions of the Customer related to the Data Processing Agreement can be addressed to the e-mail address security@jimber.io.

3.2. All questions of the Processor related to the Data Processing Agreement can be addressed to the Customer through the contact details mentioned in the header of this Agreement.

4. Rights and obligations of the Processor

4.1. The Processor acts exclusively on behalf of the Customer.

4.2. The Processor processes the Personal Data strictly in accordance with the instructions of the Customer as contained in Schedule 1 of the DPA and in accordance with the provisions of the DPA.

4.3. The Processor shall only process the Personal Data that are strictly necessary for the execution of the DPA and only the Personal Data included in Schedule 1 of the DPA.

4.4. The Processor will regularly inform and train its employees responsible for processing the Personal Data and for implementing the DPA about the provisions of privacy legislation in general and the Regulation in particular.

5. Rights and obligations of the Customer

5.1. The Customer shall, each time it issues a new processing activity to the Processor or whenever the purpose of the processing activities changes, propose an addendum to this DPA.

5.2. The Customer acknowledges and accepts its own responsibility in the event that such an addendum is not signed in time by the Parties.

6. Processing of the Personal Data

6.1. The Processor will always observe the utmost confidentiality with respect to the Personal Data processed.

6.2. The Processor will only process the Personal Data for the purposes described in Schedule 1 of the DPA.

6.3. The Customer grants the Processor permission to communicate the Personal Data to all persons, institutions and bodies that participate directly in the execution of the assignment and when this is strictly necessary for the execution of the DPA. the Processor will not transfer the Personal Data to other third parties unless this is required by or pursuant to the law or required by a court order.

6.4. The Processor may back up personal data it processes as part of the performance of this Agreement to ensure continuous service.

7. Rights of the data subject

7.1. If the Processor receives a request from a data subject whose Personal Data is being processed to exercise his/her rights in accordance with the Regulation, such as the right to object or the right to erase the Personal Data, the Processor shall inform the Customer about this order without delay.

7.2. The Processor shall, without delay and no later than within 7 working days of receiving the request, provide an appropriate response to this instruction from the Customer and either provide the requested information or make the requested adjustments to the Personal Data, or delete and destroy certain Personal Data, or inform the Customer of the reason why it is not possible to comply with the order within 7 working days.

7.3. The Customer acknowledges and accepts that in case the person concerned requests erasure of the Personal Data, the Processor does not necessarily have to remove the Personal Data from all his backups in order to give an adequate response to the order of the Customer.

8. Liability and Warranties

8.1. The Processor will strictly observe the provisions of the DPA when processing the Personal Data and guarantees to the Customer that he will take the necessary measures to ensure that his employees charged with the execution of the DPA comply with the provisions of the DPA.

8.2. The Processor guarantees in particular to the Customer that it has made its employees and appointees aware of the provisions of the DPA and has concluded an agreement with them which offers at least the guarantees expected from the Processor on the basis of the DPA.

8.3. The liability of the Processor is always limited to those cases specifically provided for in the Regulation.

8.4. The liability of the Processor shall in all cases be limited to direct damage to the following goods Customer. The Customer indemnifies the Processor at all times from all claims from third parties.

9. Duration

9.1. This DPA enters into force when the Customer registers and creates a user account on the platform of Jimber.

9.2. This DPA is concluded until the user account of the Customer is deleted on the platform of Jimber.

10. Retention of personal data

10.1. The Processor will not retain the Personal Data any longer than is necessary for the performance of the assignment for which it was provided. If the Personal Data are no longer required after this, then the Processor will exchange them adequately and remove them permanently, or return the data carriers to the Customer.

11. Security

11.1. The Processor will take the appropriate technical and organisational measures to secure the Personal Data and the processing thereof in accordance with Schedule 1 of the DPA.

11.2. The Processor will take the necessary measures to limit access to the Personal Data to those members of staff employed by the Processor who need access to the personal this Personal Data in order to execute the DPA.

11.3. If the Processor makes use of subcontractors for the execution of the DPA, the Processor guarantees that it has concluded an agreement with these sub-processors containing at least the provisions of the DPA.

12. Sub-processors

12.1. The Processor may appoint sub-processors to carry out the processing activities under the DPA.

12.2. If the Processor wishes to use a sub-processor within the meaning of this article 14, the Processor will undertake to enter into a written agreement with this sub-processor that covers at least all guarantees, obligations and liabilities arising from the DPA.

13. Data breaches

13.1. Upon discovery of a data breach, the Processor will inform the Customer within 24 hours of the discovery via telefoon or email.

13.2. The Processor will, after the discovery of a Data Breach, keep the Customer informed of the measures that have been taken to limit the scope of the Data Breach or to prevent it from occurring in the future.

14. Miscellaneous provisions

14.1. If one or more provisions of this DPA are declared null and void or become unenforceable, this shall not affect the legality, validity and enforceability of the remaining provisions of this DPA and of the DPA as a whole, in so far as they still have any effect or reason to exist.

The Parties undertake, to the extent legally possible, to replace the invalid provisions by a new provision that corresponds to the objectives and choices of this DPA.

14.2. Neither Party may transfer any rights under this DPA to third parties without the prior written consent of the other.

14.3. Amendments or changes to this DPA can only be made if they are accepted and signed in writing by both Parties.

14.4. In case of doubt as to the interpretation of a provision of this DPA, it shall always be interpreted in accordance with the provisions of the Regulation, at least in the light of the Regulation.

15. Applicable law and disputes

15.1. This DPA is governed in all respects by and shall be interpreted and construed in accordance with Belgian law.

15.2. In the event of any dispute regarding the execution or interpretation of the DPA, the Parties undertake to engage in good faith discussions with a view to resolving the dispute amicably.

15.3. If no resolution can be reached between the Parties after a reasonable period of time, the Parties shall try to settle such dispute in good faith through mediation. The parties will appoint an accredited mediator from the list of mediators of the CEPANI: www.cepani.be, before resorting to arbitration.

15.4. If the Parties do not reach a settlement through mediation, any unresolved dispute shall be settled by arbitration administered by the Body CEPANI: www.cepani.be, who will make a binding decision.

Executed and accepted by both Parties when the Customer created an account in the platform of the Processor.

Schedule 1: Overview of personal data, processing activities and processing purposes

Network Isolation

Processing Activity	Type of Personal Data	Processing Purpose
Account creation	E-mail address	To create an account
Login	Cookies stored by the user	To ensure the functioning and performance of the Network Isolation service
Login	Public key of the user	For authentication and encryption

Browser Isolation

Processing Activity	Type of Personal Data	Processing Purpose
Account creation	E-mail address	To create an account
Login	Cookies stored by the user	To ensure the functioning and performance of the Browser Isolation service
Browsing	Cookies stored by the end user	To ensure the functioning and performance of third party websites

Application Isolation

Processing Activity	Type of Personal Data	Processing Purpose
Account creation	E-mail address	To create an account
Login	Cookies stored by the user	To ensure the functioning and performance of the Application Isolation service

Schedule 2: Overview security measures

This Schedule 2 provides an overview of the security standards that the Controller imposes on the Processor:

- Firewalls of Jimber, Digitalocean and Gig.tech;
- 2 Factor Authentication;
- Secure passwords;
- Public and private key encryptions;
- IP-whitelisting;
- Access limitations.