TERMS OF USE - INTERTEK

1. PREAMBLE

INTERTEK offers a Blockchain which the USER wishes to use according to the conditions stipulated herein.

2. SUBJECT

The present TOU defines the obligations of the USER and the conditions under which the USER benefits from the rights of use granted to it.

USER must read and accept these TOU, including the Special Terms and Conditions for the Member Software in appendix 1 of this document.

These TOU detail the rights and obligations of the USER.

3. DEFINITIONS

Block(s)	means a set of Message Fingerprints from different Senders.
Validated block(s)	designates the Blocks that have passed the Validation stage and that form a chain held by each Node of the Network.
Blockchain	means the storage in a decentralized database, without a "master" record, of a fingerprint of each message sent by a sender within a network. The fingerprints are stacked into Blocks by the nodes that make up the network, and each Block Validated by a node is addressed to the other nodes that make up the network. Each node thus has all the fingerprints of all the messages sent by all the senders in the same network.
Channel, Channels	means any list(s) of recipient-readers, configurable by the sender by means of a module provided in the Member Software. When a sender sends a Message in the Network, it assigns to this Message a Channel, which determines the set of recipient-readers who will have a Read Right on this Message.
TOU	means these general terms and conditions of use applicable to the the USER, including their annex(es), and constitute a contract between the Parties
Personnel	means any natural person acting as an employee, officer, agent or representative of a USER and designated by the USER to post a Message in connection with the USER's role as Sender.
Decrypt / Encrypt	means the use of any cryptographic process using a "private key + public key" pair provided for in the Network Access Service and by means of which INTERTEK can (i) authenticate the sender of a Message and/or (ii) prove the integrity of the Data contained in Messages and/or (iii) ensure the confidentiality of Messages sent on the Network or stored in the sender's Message database.
Software Directive	means together the Directive n°91/250/EEC of 14 May 1991, the Directive 2009/24/EC of 23 April 2009 and the law n°94-361 of 10 May 1994.
Directive N. I.S	means Directive n°2016/1148 of 6 July 2016, Commission Implementing Regulation (EU) 2018/151 of 30 January 2018, "SRSI" Law n° 2018-133 of 26 February 2018, Decree n°2018-384 of 23 May 2018, Order of 13 June 2018 and Order of 14 September 2018.
Data	means any digital data (text, sound, image, etc.) contained in a Message by the will of its sender.
Read-only Right	means the right to permanent extraction, which a sender grants to one (or more) recipient(s)-reader(s) designated by a sender's channel, on the Data contained in its Messages, according to rules that the sender determines alone and under its sole responsibility. The Read-only Right allows the recipient-reader to process freely and without charge, without limitation of duration or purpose, the Data contained in the sender's Messages. The Read-only Right is exercised as from the authorization granted by the sender to one (or more) recipient-readers, i.e. at the time a Message is sent in the Network. A Read-only Right granted cannot be questioned afterwards.
Fingerprint	means a one-way cryptographic hashing process that converts a digital data file into a unique sequence of characters of a defined format. Once sent in the Network, the Fingerprint of a Message is proof for each Network Member, in the nodes, to Validate Fingerprint Blocks and to send Validated Blocks to other nodes of the Network.
DSP	means a Party that would be designated by decree as a Digital Service Provider (DSP) within the meaning of the N.I.S. Directive.
GDPR	means the EU Regulation n°2016/679 of 27 April 2016 *RGPD-GDPR* as well as the French Data Protection Act n°78-17 of 6 January 1978 as amended. For the purpose of the present, it also refers to the Directive 2002/58 EC of 12 July 2002 as amended, and any applicable regulations on the protection of personal data.
Information	means all information, of whatever nature (legal, technical, etc.) and whatever medium on which it is communicated (in writing, verbally, visually, electronically or by any other means), specific to each Party, and in particular information relating to or necessary for the performance of the TOU,

	information exchanged between the Parties prior to the conclusion of the TOU or on the occasion of its performance when such information can reasonably be presumed to be confidential: (i) whether such information is obtained directly or indirectly from the other Party's Personnel, (ii) whether such information is transmitted or made known to the other Party orally or in visible or tangible form.
LCEN	means the law n°2004-575 of 21 June 2004 for confidence in the digital economy.
INTERTEK Software	designates all the modules of the computer program that allow: - with regard to the Member Software, (i) to operate an INTERTEK node, and (ii) to make the Access Service available within the Network when the USER wishes to benefit from the functionalities relating to the role of sender and;
Client Software	means all the modules of the computer program that allow INTERTEK to provide the SaaS Service to the recipient-reader.
Member Software	Refers to the software operated in Software as a Service mode which integrates a Blockchain protocol management software under an "open source" user license and which the USER is invited to download when accepting the TOU. Member Software includes the software components made available as well as Network Access Service.
Maintenance	means the corrective and evolutionary maintenance services of the Member Software. INTERTEK's commitments under Maintenance are exhaustively defined in Appendix 1 concerning the Member Software.
Network Member	means any individual or legal entity acting in a professional capacity, who has the right to use the Member Software and that includes the Client.
Message	means any digital message containing Data sent by a sender to a node.
OSE	means a Party that would be designated by order as an Essential Service Operator (ESO) within the meaning of the N.I.S. Directive.
Party(s)	means individually a Party to this TOU, collectively the Parties to this TOU.
eIDAS Regulation	means the EU Regulation No. 910-2014 of 23 July 2014 on electronic identification and trust services for electronic transactions.
Network	means all the nodes of the Network operated by node operators having contracted with INTERTEK.
Trade Secrets	means any Information of which a Party is a legitimate holder relating to know-how, a business plan, an algorithm, a protocol, an IT architecture, a manufacturing or distribution process, and in general, any Information not publicly disclosed by a Party and benefiting from the protection provided by the legislative provisions applicable to business secrecy.
Network Access Service	means the right for USER to use the Member Software in particular to: (i) send Messages in the Network and have them converted into a Fingerprint by a node; (ii) benefit from storage and backup services on the INTERTEK Platform (a) of the Member Software and (b) of the database of its Messages; (iii) benefit from maintenance services for the Member Software under the conditions described in the Maintenance section of the Special Terms and Conditions for the Member Software - Appendix 1; (iv) to allow the treatment of its Data by INTERTEK for the benefit of the recipients-readers.
SaaS Service	means the right for the recipient-reader to use the Client Software remotely.
Digital Signature	means the set comprising (i) a public address within the Network and (ii) an indissociable public key generated by the Member Software from the private key of the USER. The Digital Signature is proof, as defined in the section Proof and Right of Use of Data, of the authentication of each network member.
Information System	means together (i) "*any device or set of devices interconnected*" via an electronic communications network "*one or more of which, in execution of a [computer] program, performs automated processing of digital data*" and (ii) "*the digital data stored, processed, retrieved or transmitted by that device for the purpose of its operation, use, protection and/or maintenance*" (N.I.S. Directive) (iii) owned or controlled by a Party and, more generally, any hardware and/or software device, internal or external to a Party's enterprise, necessary for the proper functioning of its information system (air conditioning, power supply, etc.).
Validation	designates the operation by which a node affixes its Digital Signature to a Block filled with Fingerprints, makes a Fingerprint of this complete Block and sends the whole (Block + Fingerprint of the signed Block) to the other Nodes of the Network. All the Validated Blocks form a chain held by each node of the Network.

4. CONTRACTUAL DOCUMENTS

The USER expressly agree that the contract documents herein shall consist of the following items, listed below in order of priority:

1. The present TOU;

2. The Special Terms and Conditions relating to the Member Software in Appendix 1 of this document

3. Any other document to which they have expressly wished to give a contractual value.

In the event of a contradiction between the contractual documents governing the relationship between the Parties, the document of higher rank shall prevail over the documents that follow in order of priority.

5. OPERATION OF THE INTERTEK NETWORK

5.1. Principles of a Blockchain protocol

A Blockchain protocol allows to store in a decentralized database, without any "master" record, a Fingerprint of each Message sent by a client within a Network. The Fingerprints are stacked in Blocks by the nodes that make up the Network, and each Block Validated by a node is addressed to the other nodes of the Network. Each node thus has all the Fingerprints of all the Messages sent by all the client members of the same Network.

5.2. The Network operated by INTERTEK

INTERTEK provides innovative know-how in the field of secure transfer and decentralized storage of digital data ("**Messages"**) using Member Software operated in Software as a Service mode which integrates a Blockchain protocol management software under an "open source" user license.

Using the Member Software features applicable to the node operator, the node operator that receives a Message from a client makes a Fingerprint of each Message, time-stamps the Fingerprint and sends the time-stamped Fingerprint to the other nodes on the Network, for subsequent purposes of (i) checking the integrity of the Message, (ii) certifying the date it was sent by the cleint, and (iii) authenticating its sender.

Using the functionalities of the Member Software applicable to the USER, the USER sends Messages to a Network node which, upon receipt, converts such Message into a Fingerprint, time-stamps the Fingerprint and sends the time-stamped Fingerprint to the other Network nodes, for subsequent purposes of (i) checking the integrity of the Message, (ii) certifying the date it was sent by the USER, and (iii) authenticating its sender.

The recipient-reader accesses the Messages for which it has been granted a Read Right by INTERTEK (through a Channel) and benefits from access to the SaaS Service and a right to use the Client Software. The sender's node that receives a Message sends an Encrypted copy to INTERTEK. Upon receipt of the Encrypted Message, INTERTEK will enable the decryption and then re-encryption of a Message to constitute a database specific to the USER and each recipient-reader who benefits from a Read Right from INTERTEK, so that only the USER sender and each recipient-reader with a Read Right can access their message database which only they can decrypt.

5.3. Becoming a Network Member

After acceptance of the TOU, the Network Member has online access to the Member Software via a download link that INTERTEK will provide.

When the USER decides to activate its relevant functionalities, the USER can generate his Digital Signature and his public sender address. If each Network Member can benefit from the USER functionalities, it remains free to write Messages or not, depending on the role it wishes to play in the Network.

5.4. Hosting

INTERTEK undertakes to ensure that the hardware and software of the hosting datacenter from which the Network Access Service is rendered by third party employed by INTERTEK are located exclusively on the territory of a country (i) of the European Union or (ii) of the European Free Trade Association (Iceland, Norway and Liechtenstein), which together form the European Economic Area (E.E.A.).

6. CONDITIONS RELATING TO THE NETWORK NODES

6.1. Conditions relative to the node

The Member Software defines the rules of consensus which assign to a network node the duty to proceed to the Validation of a Block as and when it receives Messages to be converted into Fingerprints from senders. In order to guarantee the neutrality of the Network, INTERTEK undertakes to ensure that no Network node, not even INTERTEK's, has priority in the Validation of Blocks. The respect of this rule of neutrality in the Validation of Blocks is an explicit essential quality of the Network operation expected by each of the network node operators. The Validation rules may not change during the execution of the TOU, except to the extent set forth in the Technical Configuration of the Network section.

The USER shall refrain from modifying the Messages it receives and the Fingerprints it calculates, as well as all the Digital Data it receives when receiving Messages, Fingerprints, Validating a Block or sending a Validated Block to the other nodes of the Network. Failure to deliberately comply with this essential condition of non-modification of received or transmitted Data will allow INTERTEK to suspend without notice, temporarily or permanently, the operation of the node used by the USER.

INTERTEK operates a node, with a technical configuration identical to that of each other node operator, for the reception of Messages, the creation of Fingerprints and the Validation of Blocks.

7. TECHNICAL CONFIGURATION OF THE NETWORK

Each Network Member, whatever its role, will have the same Member Software technical configuration as all other Network Members. For the avoidance of doubt, while the Member Software technical configuration is the same, the Network Member may have access to different Activated Components.

INTERTEK reserves the right to change certain technical aspects of the Network, the Member Software and the Network Access Service as soon as:

(i) the modifications made would allow for the improvement of the Member Software, the Network Access Service or the technical protection measures applied to Messages and/or Fingerprints and/or Validated Blocks;
(ii) the agreement on evidence between Network Members described in the Article Convention of Proof – proof and right to use data is not modified.

Any non-substantial changes to the technical aspects of the Member Software, Messages, Fingerprints, Blocks or the INTERTEK Information System shall be identified in the versioning of the updated technical architecture document accessible online from the Network Member's personal account.

Except for urgent technical measures justified by the security of the Member Software, the Network Access Service, Messages, Fingerprints, Blocks or the Information System of INTERTEK or of one or more Network Members, which must be notified by INTERTEK to each Network Member, any other substantial change in the technical aspects of the Network operated by INTERTEK shall be subject to prior acceptance by the USER.

8. SOFTWARE LICENSE AND MAINTENANCE

For the purposes of these TOU, the USER is granted a sub-license to use the Member Software and, at the Member's choice, the aspects relating to the role of the Sender when the Member wishes to benefit from the related functionalities. The conditions of use relating to the Member Software in its two components are detailed

9. CONVENTION OF PROOF – PROOF AND RIGHT TO USE DATA

9.1. Exclusion of Regulation eIDAS

The Network provided by INTERTEK constitutes a "*closed system*" resulting from an "*agreement between a defined group of participants*" within the meaning of article 2.2 of the eIDAS Regulation. The eIDAS Regulation therefore does not apply in any way to these TOUs, a fact which the Network Member acknowledges by accepting the TOU.

9.2. Governance of Network

INTERTEK gives the undertaking that the technical rules for the operation of the nodes and the legal rules for the operation of the Network will not change at the sole instigation of INTERTEK, except to the strict extent fixed in the article Technical Configuration of the Network.

9.3. Digital Signature Management

The management of the authorizations of the Personnel of each Network Member for :

(i) use of the Member Software; and
(ii) the use of the Network Member's Digital Signature; and
(iii) the use of the SaaS Service and the Client Software for the recipient-readers;

is provided by the USER under its sole responsibility.

Under no circumstances may INTERTEK cause the suspension or medication of the use of a Network Member's Digital Signature, either temporarily or permanently, or require the USER to create a new Digital Signature with a new private key EXCEPT to ensure (i) the security of the Network for the benefit of other Network Members or Information System provided by INTERTEK and (ii) compliance with the contract on the evidence set out in this article, such as in the event of:

(i) loss by the USER of its private key; or
(ii) manifestly fraudulent use of the USER's private key or public address by one of its Personnel or by a third party, even if mandated by the USER concerned; or
(iii) inability of the USER to prove possession of the private key linked to the public key attached to its public address.

9.4. Convention of Proof

By using the Software made available by INTERTEK, each Network Member acknowledges that it has entered into a "*contract relating to proof... on rights which the parties have free disposal*" (art.1356 Civil Code) intended to give evidentiary value to each Message, as regard:

(i) the authentication of the sender of this Message through the use of his Digital Signature; and
(ii) the identification of the recipient(s)-reader(s) benefiting from a Read-only Right on this Message and on each Message from a sender defining the detailed list of recipient-readers to whom this sender grants a Read-only Right;
(iii) the Data contained in each Message, by integrity check between (a) the Fingerprint of such Message contained in the Network and (b) the corresponding Message contained in the Message database of the sender or a recipient-reader, and
(iv) the date and time of submission to the Network of the Fingerprint of a Message by a Network Node, and
(v) the date and time of Validation of the Block containing the Fingerprint of this Message by a Network Node.

The contract relating to proof applies, between INTERTEK and each Network Member, under strictly identical conditions, to Messages for which INTERTEK is the sender and to Blocks that are Validated by the node operated by INTERTEK.

BY ACCEPTING THE TOU, INTERTEK AND THE USER EXPRESSLY ACKNOWLEDGE, AS DO EACH OF THE OTHER NETWORK MEMBERS UNDER STRICTLY THE SAME CONDITIONS, THAT :

(i) each Message and the Data contained therein constitute a "*writing*" within the meaning of Article 1365 of the Civil Code ;

(ii) the use of the cryptographic process implemented in particular by the INTERTEK Software and which allows the creation of a unique Digital Signature specific to each Network Member, inseparably linked to the Message of its sender and of which a Fingerprint is contained in the Network:

a) "*consists in the use of a reliable identification process guaranteeing its link"* with the Message used for the realization of its Fingerprint (article 1367 al.2 of the Civil code);
b) allows for the reliable authentication of the Network Member who uses it and constitutes a *"signature necessary for the perfection of a legal act [which] identifies its author*";
c) allowing each Network Member concerned to "*express its consent to the obligations arising therefrom*" within the meaning of Article 1367 of the Civil Code;

(iii) the comparison of a Fingerprint with the Message stored in the database of the Messages of a sender or a recipient reader, and converted into a new Fingerprint using the same cryptographic hash process as the one contained in the Software made available by INTERTEK, enables to guarantee the integrity of the Data contained in this Message;

(iv) each Validated Block, a complete and strictly identical copy of which is distributed to each network node, and the database of the Encrypted Messages of each sender and of each recipient reader together constitute a means of storing each Message and the Data contained therein "*of such a nature as to [...] guarantee the integrity*" of the Message sent into the Network by its Sender (article 1365 of the Civil Code) ;

(v) the time-stamp of the recording by a node of the Fingerprint of a Message is worth proof of the date and time of the sending by the sender of the Message in the Network;

(vi) in general, the writing represented by each Message associated with a Digital Signature and its Fingerprint have evidential value with respect to each Network Member (a) of the Data contained in each Message, (b) of the time-stamp of the sending of each Message by its sender and (c) of the authentication of the sender of each Message

9.5. Guarantee of the integrity of the Data

Network Members acknowledge that the Data is incorporated into a Message under the sole responsibility of the sender of the Message concerned. The sending of a Message converted into a Fingerprint in the Network does not allow the sender, INTERTEK or any other Network Member to affirm or guarantee that the Data of a Message is "true" or "exact", but establishes the proof that this Data was integrated into a Message and sent in the Network by the sole will of its sender and that the Data of each Message constitutes proof between the Network Members in accordance with the article Convention of Proof – proof and right to use data.

10. CONDITIONS RELATING TO THE SENDER ROLE

10.1. Conditions relating to the Databases of the Network Member as a sender

10.1.1. The sender is the producer of the content of the database of its Messages

The sender declares that it has made investments that give it the status of database producer within the meaning of Article 7.1 of the Database Directive (art. L.341-1 IP Code) with respect to the Data contained in the database of Messages, a Fingerprint of each Message of which is contained in the Network. In this respect, the sender prohibits each Network Member other than the recipient-reader(s) that it designates:

(i) any extraction and/or reuse of all or any qualitatively or quantitatively substantial part of the Messages and the Data contained in the database of its Messages, and

(ii) any repeated and systematic extraction or reuse of qualitatively or quantitatively insubstantial parts of the Messages and/or Data contained in the database of its Messages when such operations manifestly exceed the conditions of normal use of the database of its Messages set out in the contract.

By express agreement, the USER, when acting as a sender, authorizes INTERTEK, at its request or at the request of a recipient-reader benefiting from a Read-only Right, to extract and/or reuse all or part of the Data contained in its Messages for evidential purposes within the meaning of the Proof and Right of Use of Data article herein.

10.1.2. Granting of an extraction right to INTERTEK

In order to enable INTERTEK to perform the INTERTEK Network Access Service, the USER and each recipient-reader grant INTERTEK, or a party appointed by INTERTEK, a non-exclusive and free right to extract and/or re-use all of their Messages, including the Data contained therein, for the following purposes

(i) allow each Message and the Data contained therein to be used as evidence between the Network Members as stated in the article Evidence and right of use on the Data of the TOU;
(ii) monitor the security of the Information System and the Member Software made available by INTERTEK;
(iii) improve the technical operation of the Member Software;
(iv) perform the services comprising the INTERTEK Network Access Service, in particular to enable INTERTEK (a) to create, in the name and on behalf of the USER and a recipient-reader, a database of Messages, each of which shall be the producer/manufacturer within the meaning of Article 7.1 Data Base Directive and (b) to fulfil the obligations agreed between INTERTEK and a recipient-reader benefiting from a Read-only Right granted by the USER;
(v) offer new services.

10.2. Sender and Contributor

A sender may decide to open write access to one of its nodes to one or more Contributors that it chooses freely. The opening by a sender of a right to write to a node for the benefit of a Contributor may be done either by the use of a Network access management module offered by the Member Software, or by a software module developed by INTERTEK when acting as a sender, itself alone. In the latter case, only the USER shall be liable for any malfunction (i) of the Contributor's Network access module or (ii) misuse of this module by the Contributor.

The assignment of a "Contributor" profile to any professional chosen by a sender is made under the sole and entire responsibility of the sender concerned and implies acceptance by this sender of the fact that the Messages of this Contributor shall be considered as proof within the meaning of the article Convention of Proof – proof and right to use data of the TOU with regard to him as well as with regard to the other Members of the Network insofar as the Messages of the Contributor benefit from the Digital Signature of the Sender.

The principal sender shall be responsible for the strict compliance of its Contributor(s) with the TOU, including their annex(es). It is the responsibility of the USER, when acting as a sender, concerned to contract directly with each Contributor to define the rights and obligations incumbent on the Contributor in respect of write access to the Network. Besides, it shall be the USER’s responsibility to secure the consent of its Contributors to publish their personal information in the Member Software.

10.3. Designation of recipient(s)-reader(s)

Once its Digital Signature has been created, the USER writes a Message and designates, if it so wishes, the recipient(s)-reader(s) who can read the Data contained in its Messages, in a provisional or definitive manner according to the settings of the Member Software which it operates alone and under its sole responsibility. The choice of a recipient-reader cannot be made retroactively by a sender on Messages already sent in the Network.

10.4. Terms and Conditions for Messages

1.1.1 Nature of the Message - the Message is not Private Correspondence

The USER warrants that its Messages will not contain any Data of a private nature between two identifiable natural persons but only and exclusively Data (i) purely technical related to the professional activity of the sender and/or its recipient-readers. Therefore, the parties acknowledge and accept without reservation that neither a Message nor its Fingerprint constitutes a "correspondence" related to the private life of an identifiable natural person but a "*communication*" by electronic means within the meaning of Article 1 of the LCEN to a category of professional public "*which does not have the character of a private correspondence*".

Consequently, the USER expressly acknowledges that neither INTERTEK nor any other Network Member shall infringe the confidentiality of correspondence when INTERTEK or any of the Network Members (i) receives or transmits Messages or Fingerprints and (ii) stores Messages in a Message database, or (iii) processes, on behalf of a recipient-reader, the Fingerprints and/or Data contained in Messages for which this same recipient-reader benefits from a Read Right granted by a sender.

1.1.2 The Message Must Not Contain Any Personal Data

The purpose of the Network Access Service is also to enable the integrity of the Data contained in each Message to be checked by comparison with the Fingerprint that is sent and kept in the Network. INTERTEK reminds the USER that the Data contained in each Message are purely technical data, possibly relating to the execution of a contract concluded directly between a sender and a recipient-reader and independent of the Network Access Service provided by INTERTEK.

If a Message concerns Data collected about a consumer who is purchasing a product or service from a recipient-reader or who wishes to obtain information about the latter's products or services before purchasing them, the Client may, in particular and without limitation, include in its Message:

(i) any data relating to the date/time of purchase by the consumer ("when");
(ii) any data relating to the location of the product sold/service rendered ("where");
(iii) any data related to the product sold/service rendered ("what").

Except with the informed, prior and written consent of the natural person concerned, or on another legal basis allowing such information to be collected and processed (following a documented legal analysis), the **USER expressly undertakes not to include in the Data contained in any Message any data that would allow the direct or indirect identification of a natural person within the meaning of the Legislation on personal data, in particular the GDPR, provided that if the USER includes any data that would allow the direct or indirect identification of a natural person the USER does so with the express consent of the data owner and according to all legislative requirements of the data owner's jurisdiction**. It shall be the USER's obligation to collect such consent from the data owner and local authorities. The respect of this commitment by each sender constitutes an explicit essential quality of the sender's service expected by INTERTEK and by each recipient-reader.

In the event that the USER should fail to comply with this explicit essential quality, the USER in default shall be solely responsible for all the consequences, in particular financial consequences (damages, administrative or criminal fines, etc.), and undertakes to indemnify and hold harmless, without any limitation whatsoever, INTERTEK and each of the other Network Members from the consequences of its failure to comply with the present terms and conditions, which may be borne by INTERTEK and/or each Network Member concerned.

11. INTERTEK'S ROLE - SUPPLIER OF ENCRYPTION MEANS AND SERVICES

Within the framework of its obligations hereunder, INTERTEK is not a provider of "*electronic certification services*" within the meaning of the LCEN, nor is it a provider of "*means of electronic identification and trust services*" within the meaning of the eIDAS Regulation.

For the Network Access Service and for the services of creating Digital Signature and converting Messages into Fingerprints by the Software, INTERTEK makes available means and/or services of cryptology "*ensuring exclusively functions of authentication or integrity control*" and has facilitated proceeding to the preliminary declaration of this service to the National Agency for the Security of Information Systems (art.30 II LCEN and art.3-3° decree n°2007-663 of 2 May 2007).

12. LIABILITY AND INSURANCE

USER shall be liable for and shall indemnify INTERTEK from immediate, direct and foreseeable damages caused by a partial or total failure to perform its obligations stipulated herein.

IN NO EVENT SHALL INTERTEK BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY THE USER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE, EVEN IF INTERTEK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF SUCH DAMAGES WERE FORESEEABLE, WHETHER ARISING FROM YOUR ACCESS TO OR USE OF THE Client Software, OR OTHERWISE. INTERTEK'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000). THE TERMS OF THIS PARAGRAPH 12 SHALL BE ENFORCED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

13. PERSONAL DATA

Each Party is responsible for processing the personal contact data of the other Party's Personnel that each Party collects directly (art.13 GDPR) from the other Party in the course of performing their relevant obligations for the following purposes only:

(i) processing necessary for the execution, verification, maintenance, invoicing and collection of sums due under the contract concluded between INTERTEK and the USER and for the management of Digital Signatures and login credentials of the Member's Personnel to the Member Software (art.6.1 (b) GDPR) ;
(ii) processing necessary for the legitimate interests of securing the Software provided by INTERTEK and/or the Network Access Service and/or the Information System provided by INTERTEK (art.6.1 (f) GDPR);
(iii) processing necessary for the legitimate interests of each Party (art.6.1 (f) GDPR) for the purpose of prospecting for its other products or services with a free and immediate unsubscribe link integrated into each mailing in electronic format to the Personnel of the other Party

Each Party shall retain the personal data of the other Party's Personnel for the duration of the retention and, beyond that, for the period necessary for the exercise of any legal action that may be brought between the Parties in connection with any dispute relating to the performance of their relevant obligation herein. At the end of the statutory period of limitation for legal action in France (or in the jurisdiction of the data subject), the personal data of the Personnel shall be deleted from the electronic databases of the Party processing them.

Each member of the Personnel of a Party has rights under the personal data legislation and in particular a right of access (art.15 GDPR) and rectification (art.16 GDPR) on his personal data processed by the other Party by sending an email to the email address GDPR@Intertek.com. Each Party undertakes to process requests under these rights in accordance with the legislation on personal data.

It is the responsibility of each Party to inform its Personnel of the existence of the processing of their personal data by the other Party and of the rights offered by the other Party under the legislation on personal data.

Any possible subcontracting by a Party of the technical management of its Personnel's database will be the subject of a written contract between this Party and its subcontractor, the data controller undertaking to ensure that its subcontractor strictly complies with the rules of protection of the personal data of the Personnel of the other Party and guarantees their security and confidentiality.

Each Party undertakes to inform the other Party, without delay after becoming aware of it, of any known breach of the other Party's personal data that it processes under this Article, (i) regardless of the size of the breach and (ii) regardless of whether the data subject to the breach is encrypted.

14. INTELLECTUAL PROPERTY

Members of the Network are reminded that all elements (texts, images, logos, trademarks, domain names, databases, software...) licensed, developed or held by INTERTEK are protected by intellectual property rights and may not be reproduced or used without the prior authorization of INTERTEK.

No one is authorized to exploit, distribute or use the intellectual property rights including, but not limited to, the rights held in the INTERTEK name or in the Member Software and Client Software, without the prior written consent of INTERTEK.

Any use without the authorization of INTERTEK or in violation of these TOU, including their annex(es), therefore constitutes an infringement.

For the avoidance of doubt, all intellectual property rights relating to the Software or the SaaS Service made available by INTERTEK is and shall remain the exclusive property of INTERTEK or the main licensee with whom INTERTEK may have a separate contract.

15. OSE and DSP

In the event that a Party is (i) designated by decree as an Essential Service Operator (ESO) or (ii) a Digital Service Provider (DSP) within the meaning of the NIS Directive Directive, the Party concerned undertakes to:

(i) inform the other without delay;
(ii) to implement, at its own expense, all appropriate security measures imposed by the N.I.S. Directive, in particular to prevent any incident that compromises the security of the Information System (including digital data) used by the Party concerned;
(iii) to declare to the ANSSI any incident affecting its Information Systems to the extent imposed by the N.I.S. Directive.

16. CONFIDENTIALITY – TRADE SECRET

16.1. Non-disclosure of Information

Each Party undertakes, on its own behalf and on behalf of its Personnel, to ensure the protection of the strictest confidentiality concerning the use of Information, including Trade Secrets, received from the other Party throughout the duration of the TOU.

Each Party agrees:

(i) to ensure that each of its Personnel who have access to Confidential Information has signed a confidentiality agreement with obligations equivalent to those set forth in this section or is bound by professional secrecy under applicable law; and
(ii) to justify this commitment in writing and without delay at the first request of the other Party.

The Party receiving Information from the other Party undertakes to keep it strictly confidential and to protect and treat it with the same degree of care as it accords to its own Information. To this end, the receiving Party will ensure that such Information :

(i) are transmitted only to its Personnel having to know about it;
(ii) not be copied, reproduced or duplicated in whole or in part, if such copies, reproductions or duplications have not been previously authorized in writing by the Party from which they originate;
(iii) may be disclosed to a third party only with the written consent of the transmitting Party and the execution of a confidentiality agreement between such third party and the receiving Party containing obligations identical to those contained herein.

Each Party that becomes aware of any unauthorized disclosure or use of the other Party's Information or any breach of the TOU will promptly notify the other Party and will cooperate with the other Party to stop the unauthorized disclosure or use of such Information.

16.2. Exceptions to Non-disclosure

The Party receiving Information, including Trade Secrets, shall be relieved of its non-disclosure obligations with respect to any Information for which it can provide prior written evidence that:

(i) the Information concerned has fallen into the public domain in the absence of any fault or breach of contract, whether intentional or unintentional, attributable to it; or
(ii) the Information concerned was already known to him/her previously, having been received from a third party in a lawful manner; or
(iii) the disclosure of the Information concerned has been authorized in writing by the Party from which it originates.

Each Party acknowledges that any unauthorized use or disclosure of the other Party's Information shall give rise to contractual liability under this TOU.

16.3. Legal Obligation to Disclose

In the event that a Party is required to disclose Information pursuant to a legal obligation or pursuant to a decision of a judicial or administrative authority, it undertakes to inform the other Party without delay, unless expressly prohibited by law, so that the other Party can protect the confidentiality of its Information as far as possible.

16.4. Exchange of Information

Nothing in these TOU shall be construed to require either Party to transmit to the other any Information, including Trade Secrets.

Each Party shall transmit to the other only such Information as the transmitting Party deems necessary.

Neither Party warrants the truth or accuracy of the Information disclosed, but agrees to provide it in good faith, based on its knowledge at the time of disclosure.

Each Party acknowledges that any use by it of the Information, including Trade Secrets, of the other Party, or any disclosure of such Information to third parties is likely to cause serious harm to the Party that transmitted it. Consequently, each Party shall refrain from any use, direct or indirect, of all or part of the Information during the term of the Contract, except for its own benefit and solely with a view to the performance of the Contract, with the exception of any other use, private or public.

This undertaking by each Party not to re-use the other Party's Information, including its Trade Secrets, is a substantial and determining condition for each Party to communicate Information to the other, and failing which each Party would have refrained from communicating such Information to the other. Any failure, whether voluntary or involuntary, by a Party to comply strictly with its non-reuse and confidentiality undertaking shall constitute a manifestly unlawful disturbance for the other Party.

16.5. Non-disclosure of Fingerprints by node operators

For the proper functioning of the Blockchain, the node operator undertakes to keep the confidentiality of the Fingerprints, without any time limit after the effective end of the use of the Member Software by the node operator, and not to make use of them after the end of the Contract, nor to make the Fingerprints public, for any purpose whatsoever.

17. TERMINATION

17.1. Explicit Essential Quality and Exception of Non-Performance

INTERTEK may immediately and automatically suspend the performance of its services and in particular the license to use the Member Software, and the Network Access Service (a) in the event of sufficiently serious or repeated non-performance of its obligations by the USER or (b) in the event of non-compliance by the USER with an explicit essential quality of its service, in particular:

(i) the strict respect of INTERTEK's intellectual property and trade secrets and the conditions under which INTERTEK grants the USER the right to benefit from the Network Access Service and/or to use the Member Software;

(ii) strict compliance with the conditions of storage or use by the USER of the elements making up its Digital Signature (private key, private address, etc.) against any risk of compromise, loss, etc.

17.2. Restitution of Messages

INTERTEK undertakes to return to the USER (or the recipient-reader), free of charge, a copy of all the Messages contained in the database of its Messages, and not to exercise any right of retention on these Messages, for whatever reason. The Messages are returned free of charge to the USER (or to the recipient-reader) in a standard format which does not require the use of the INTERTEK Software to be reused.

Within thirty (30) days following the effective date of termination of the TOU, regardless of the cause, the USER (or recipient-reader) undertakes to recover the Data using the function provided for this purpose in the Software. If the USER (or the recipient-reader) has not proceeded with this export within thirty (30) days of the effective date of the termination of the Contract, whatever the cause, INTERTEK shall proceed with a complete export of the Client's (or the recipient-reader's) Data which INTERTEK shall store in an Encrypted manner and keep inactive on an external medium for a period of ninety (90) days and shall inform the USER (or the recipient-reader) thereof in writing. If the USER (or the recipient-reader) fails to request the return of its Data to INTERTEK within this period, INTERTEK shall be entitled to proceed with the definitive deletion of the USER's (or recipient-reader's) Data.

The operation of a blockchain protocol prevents by nature the deletion of any Fingerprint integrated in a Validated Block sent to the Network, which is recognized and accepted by each Network Member. Therefore, once the full copy of all Messages has been effectively returned by INTERTEK to the USER (or the recipient-reader) and stored in the USER's (or the recipient-reader's) Information System, under its sole responsibility, the Messages converted into Fingerprints will be kept in the Network, without the Data contained therein being able to be reconstituted in a form that can be read by anyone.

No service other than the full return to the USER (or to the recipient-reader) of all the Messages contained in its Message database shall be provided by INTERTEK under the terms of reversibility, INTERTEK being under no obligation to ensure any continuity of the service provided thanks to the INTERTEK Network Access Service, this absence of continuity of service constituting (i) decisive information for INTERTEK's consent to render the Network Access Service to the USER (or to the recipient-reader) and (ii) an explicit essential quality of the service rendered by INTERTEK to the USER (or to the recipient-reader) under the present terms.

18. FORCE MAJEURE

Neither Party shall be liable for failure to perform any of its contractual obligations due to the occurrence of an event of force majeure, which is defined as an event (i) beyond the control of the Party experiencing it (ii) which could not reasonably be foreseen at the time of the conclusion of this TOU (iii) and the effects of which cannot be avoided by appropriate measures.

For the duration of the force majeure event, if the impediment is temporary (less than thirty (30) days), the force majeure event shall suspend the performance of its obligations by the Party invoking it, unless the resulting delay justifies the termination of the contract formalized herein (except for the obligation to pay the contractual sums due on the date of occurrence of the force majeure event)

If the impediment is definitive or of more than thirty (30) days, the contract shall be terminated and the Parties released from their obligations, subject to notification of such termination by the more diligent of the two Parties. In all cases, the Party affected by the force majeure shall take appropriate measures to avoid, eliminate or reduce the causes of the delay and resume the performance of its obligations as soon as the event invoked has disappeared.

19. APPLICABLE LAW AND JURISDICTION

These TOU are subject to French law, both for the rules of form and substance. In the event that the TOU are translated into a foreign language, only the English version shall be deemed authentic between the Parties.

In the absence of an amicable agreement between the Parties for any dispute relating to the interpretation, execution or termination of the contract, the Commercial Court of Paris is expressly assigned to the case, even for summary proceedings.

Appendix 1 - Special Terms & Conditions - Member Software

1 MEMBER SOFTWARE LICENSE

1.1 Modules Composing the Member Software

The Member Software implies for each of the Network Members, a right to use the components of the Member Software related to the role of node operator and entails the application of the rights and obligations related thereto. In addition to these aspects common to all Network Members, the Member Software implies, for those Network Members who have activated the functionalities relating to the role of sender, to benefit from the rights and obligations associated with this role.

1.1.1 The Member Software thus Includes Modules Applicable to All Network Members, Covering the Role of node operator:

(i) a module to create a Network Node ;
(ii) a module allowing you to create and manage your Digital Signature and your public node address within the Network;
(iii) an *Application Programming Interface* (API) module allowing the node to receive Messages and to send a Fingerprint of each Message to the other nodes of the Network in a secure and time-stamped manner.

1.1.2 It Also Includes, for Network Members Choosing to Use the Functionalities Relating to the Sender Role :

(i) the functionalities associated with the API allowing the sender (including its Contributors) (a) to send Messages in one of the nodes it operates and to send a copy of each Encrypted Message to INTERTEK (incoming API) and (b) to have access to the database of its Messages;
(ii) software modules of the "*software development kits*" (SDK / toolboxes) for the development of mobile applications and web applications (portals, data exposure front-ends, etc.);
(iii) a web portal for viewing the Messages in the sender's Message database and for matching its Messages with the corresponding Fingerprints made by its node;
(iv) a module allowing the sender to manage its Channels, i.e. the list of recipient-readers to whom the sender grants a Read Right on the Data contained in its Messages;

1.2 Delivery and Installation of the Member Software

The Member Software can be downloaded from a URL link provided by INTERTEK. It is the sole responsibility of the Network Member to ensure the installation of the Member Software in its Information System according to the indications provided by INTERTEK.

As regards the modules relating to the role of the sender (cf. 1.1.2 above), from the date of acceptance of the TOU, and provided that the Network Member has activated the sender functionalities, they are licensed by INTERTEK to the sender, in executable version only, and only under the conditions restrictively described in this Member Software User License.

1.3 Limits of Use of the Member Software

From the date of acceptance of the TOU by the Network Member, as a node operator and, if applicable, as a sender, the Member Software is sublicensed by INTERTEK to the Network Member only (i) in executable version, (ii) for the duration of the TOU and (iii) under the conditions described in this article.

Open source software components incorporated into the Member Software are licensed to the Network Member in accordance with the text of the open source license attached to each such software component.

The right to use the Member Software is granted by INTERTEK to the Network Member on a personal basis. The Network Member shall refrain, directly or indirectly with the help of a third party, from carrying out any operation enabling it or a third party to use the Member Software, and when the functionalities relating to the role of Sender have been activated, the Network Access Service, the Messages, the Fingerprints, the Blocks or the Information System provided by INTERTEK, except within the limits set out herein, and shall therefore refrain from

(i) allow any third party to have access to all or part of the Member Software and when the functionalities relating to the role of sender have been activated, the Network Access Service, the Messages, the Fingerprints, the Blocks or the Information System provided by INTERTEK;
(ii) use the Member Software, and when the functionalities relating to the role of sender have been activated, the Network Access Service, the Messages, the Fingerprints, the Blocks or the Information System INTERTEK in a manner not provided for herein, in any practical, technical or legal manner whatsoever;
(iii) assign, lease, lend, encumber, transfer or make available to a third party, whether free of charge or against payment, by any technical, practical or legal means whatsoever, all or part of the Member Software and, where the functionalities relating to the role of sender have been activated, the Network Access Service, the Messages, the Fingerprints, the Blocks or the Information System provided by INTERTEK.

1.4 Right to Correct the Member Software

In accordance with the Software Directive (art. L.122-6-1 1° al.2 IP Code), INTERTEK reserves the exclusive right to correct or cause to be corrected any malfunctions of the Member Software, in particular those that prevent the Network Member from using the Member Software in accordance with its intended purpose. INTERTEK's commitments to correct or caused to be corrected malfunctions in the Member Software are exhaustively defined in the Maintenance article. Consequently, the Network Member is prohibited, alone or with the assistance of a third party, from modifying, adapting or creating variants of all or part of the Member Software, for any purpose whatsoever.

1.5 Evolution of the Member Software Functionalities

INTERTEK reserves the right to freely develop the operation and/or functionality of the Member Software, including corrective or preventive Maintenance as described in the Maintenance article, insofar as this development :

(i) does not remove any functionality from the Member Software previously used by the Network Member, and
(ii) complies with the technical commitments of INTERTEK set out in the article Technical configuration of the Network of the TOU.

1.6 Management of Personnel Identifiers

The node operator undertakes to take all necessary measures to keep secret the connection identifiers of its Personnel to the Member Software and not to disclose them in any form whatsoever. The Network Member is solely responsible for the use of the identifiers, which it alone is responsible for assigning, keeping, modifying, withdrawing and/or invalidating and managing.

In the event that the Network Member becomes aware that an unauthorized person has access to the Member Software, in any way whatsoever, the Network Member undertakes to inform INTERTEK without delay.

1.7 Member Software Export

It is the responsibility of the Network Member to ensure that:
(i) the Information System in which it installs the Member Software is not located on the territory of a country that is subject to an official embargo or export and/or use ban adopted by the European Union or France;
(ii) no Personnel may access the Member Software from the territory of a country that is subject to an official embargo or ban on export and/or use adopted by the European Union or France.

The Network Member undertakes to fully and unconditionally assume and guarantee the consequences, in particular the financial consequences (fines, penalties, damages, etc.) of such a breach which may be charged to INTERTEK.

1.8 Explicit Essential Qualities to be Met by the Network Member

The Network Member's strict compliance with the terms and conditions under which INTERTEK grants it the right to use the Member Software under this Member Software License Agreement, constitutes the essential qualities of the service to be provided by the Network Member that are expected by INTERTEK

Any modification or attempted modification by the Network Member of the conditions of access to or use of the Member Software under conditions not provided for herein, without the prior written consent of INTERTEK, represents a considerable danger to the continuity of INTERTEK's business, whose Trade Secrets and intellectual property on the Member Software constitute essential assets.

Accordingly, any modification or attempted modification of the terms of use of the Member Software, whether voluntary or involuntary, by the Network Member, shall be deemed to constitute a sufficiently serious breach by the Network Member to entitle INTERTEK to:
(i) immediately and automatically suspend the right to use the Member Software, without notice or formality of any kind and/or
(ii) terminate the TOU, including the annexe(s), due to the urgency and seriousness of the breach, with immediate effect and without prior notice.

2 MAINTENANCE

2.1 Obligations of the Network Member

In order to benefit from the operation of the Network and from Maintenance services on the Member Software, the Network Member is required to update its Information System as and when workarounds, updates and/or new versions of the Member Software are made available by INTERTEK. If, when a workaround, update or new version of the Member Software is made available, the Network Member's Information System is not compatible with this workaround, update or new version, the Network Member undertakes to inform INTERTEK as soon as this incompatibility is detected and to find, with INTERTEK, a specific solution to resolve, as far as possible, the problem encountered.

The Network Member undertakes to inform INTERTEK without delay of any changes in the configuration of its Information System which could jeopardize the proper functioning of the Network and/or the Member Software, Messages, Fingerprints, Blocks, INTERTEK's Information System or the performance by INTERTEK of Maintenance under the conditions stipulated herein. If INTERTEK is not previously informed of these changes, INTERTEK shall not be liable for any possible malfunction of the Node operated by the Network Member.

In general, the Network Member assumes responsibility for the physical and logical security of (i) the terminals used to access the Member Software and the Network Access Service (computer, smartphone, tablets, etc.) and (ii) its Information System in which it installs the Member Software. In the event that the Network Member becomes aware that an unauthorized person has access to the Member Software, the Network Member undertakes to inform INTERTEK without delay.

2.2 Scope of Member Software Maintenance

To benefit from the Member Software Maintenance, the Network Member is required to:

(i) report as soon as possible to INTERTEK any malfunction of the Member Software and transmit without delay to INTERTEK any information necessary to enable INTERTEK to locate and reproduce the said malfunction;
(ii) make themselves fully available to INTERTEK and allow INTERTEK to contact any other person likely to provide any useful information on the reported malfunction in order to ensure its reproduction and correction.

INTERTEK undertakes to inform the Network Member without delay of the availability of a workaround, an update or a new version of the Member Software in execution of its obligations under the Maintenance. The Network Member concerned then undertakes to access by any means proposed by INTERTEK to the corresponding software element and to install it without delay in its Information System.

Any formal notice by INTERTEK to produce a workaround, an update or a new version of the Member Software (i) which is not complied with by the Network Member and (ii) which is not justified in writing by an objective reason, may result in the immediate suspension by INTERTEK of the right to use the Member Software. This commitment is an explicit essential quality of the Network Member's performance expected by INTERTEK.

INTERTEK will use its best efforts to remedy any anomalies, errors, bugs or latent defects that may affect the Member Software.

The Network Member nevertheless acknowledges that INTERTEK remains dependent on the state of the art of software technology so that it cannot be guaranteed that INTERTEK will be able to correct all possible anomalies, errors, bugs or hidden defects that may affect the Member Software. In accordance with art.1133 al.3 of the Civil Code, by accepting this TOU, the Network Member expressly declares that he/she accepts the inherent randomness of software development and operation techniques, and therefore waives any dispute based on an error relating to the quality of the Member Software.

As soon as INTERTEK reproduces a malfunction, INTERTEK undertakes as soon as possible to install in production any temporary workaround solution, update or new version of the Member Software that will resolve any malfunction of the Member Software and/or the Network Access Service. The present terms and conditions, including the right to use the Member Software, apply to any temporary workaround, update or new version of the Member Software.