LEGAL NOTICE AND TERMS OF USE FOR IDENTIFICATION VERIFICATION

1 General Provisions

mesoneer AG ("mesoneer") provides a service whereby official identity documents (e.g. passports, identity cards and drivers' licences) ("Identity Documents") are verified and, where applicable, matched with the person they have been issued to ("you" or "Applicant"). mesoneer provides this service for its customers, e.g. financial institutions, insurance companies, online platforms, car sharing providers, car hire companies, entertainment platform operators and signature providers ("Partners") in order to comply with legal requirements or to increase security with respect to the identity of their end-users. In this context, mesoneer acts on the basis of contracts with its Partners, according to their instructions and in accordance with relevant regulatory and statutory requirements – the identification services are provided by mesoneer for and on behalf of the Partner and without you being under any obligation to pay mesoneer. The contractual terms and conditions agreed between you and the respective Partner shall apply exclusively to the Partner's services and also to any payment of the costs incurred in connection with the identification. There is no direct contractual relationship between you and mesoneer.

mesoneer employs the services of Electronic Identification, S.L. ("Solution Partner" or "eID"), Avenida Ciudad de Barcelona 81, 28007 Madrid, to perform the identification process, which is eIDAS certified and complies with the provisions of the General Data Protection Regulation (GDPR). Therefore, in addition to these Terms of Use, you must also comply with the "Certification Practice Statement" ("CPS") and the "Privacy Policy" issued by eID and included in the service.

By using this service, you acknowledge that you have read, understood and agree to accept this Legal Notice and Terms of Use including the Notices of eID. If you do not agree with these terms and conditions, please refrain from using the service.

2 How Video Identification Works

The following outlines how the entire video identification procedure works. Depending on the Partner's use case, the entire procedure or only parts of it may apply as outlined.

Part of the service consists of a video identification procedure or an asynchronous video conferencing procedure, which facilitates unsupervised remote video identification in real time, records the entire procedure of registering a person and enables remote validation of identity documents via the video recording.

The procedure comprises two parts, an automatic module where several security checks are performed on the document presented during the video recording, as well as a biometric facial comparison between the person presenting the document, the user, the user's photo and a liveness detection and precise data extraction.

All of this information is used to support a decision by a human staff member employed by mesoneer's Solution Partner who will subsequently review the entire video recording asynchronously and decide whether or not an identity can be attributed based on the documentation presented. The staff member of the Solution Partner functions in this connection as a Registration Authority (RA).

The technology used automatically detects security features such as patterns, insignia and optically variable elements in real time.

3 Elements of the Video Identification Procedure

The video identification procedure is conducted on the basis of the following elements:

- Text and spoken instructions for the Applicant.
- Automatic management of surroundings (lighting, network, camera settings), enabling an optimal recording of the identification video and documentation.
- Image comparison with original documents using pattern matching technology to verify the authenticity of the documents.
- Data extraction (OCR) of documents' MRZ and the possibility to retrieve credentials in real time.
- Verifying that the front and the back of the document are identical (where applicable).
- Biometric registration of the person and real-time comparison with the photograph on the identity document.
- Registration Authority verification tool to have the procedure checked by a qualified person

who has previously received specific training for this purpose.

Once you, the Applicant, have selected the identity document that you intend to use to carry out the procedure, an application-driven streamed video recording is generated in which you present the front and back of your identity document for real-time identification and validation. You will also be asked to show and scan your face to enable automatic biometric recognition.

For the subsequent asynchronous verification by a human agent, a security log is created that contains the evidence obtained during the procedure and records which evidence could not be provided or could not be provided in full. Each step in the entire procedure is time-stamped.

The identification procedure records the entire verification chain from collecting the evidence during the video identification to the subsequent verification by the Registration Authority. The result is a verified identity comprising technical security that is equivalent to identification in the presence of other people.

4 Starting the Identification Procedure

Before the video identification procedure is started, you will be provided with summarised information that you are about to initiate a remote video identification procedure, the purpose of which is to issue a certificate to a natural person.

The Applicant must then read and accept these Terms and Conditions for the video identification procedure and agree to the processing of the biometric data required to carry out the procedure. To this end, the Solution Partner will provide the Applicant in advance with its privacy statement governing the processing of personal data during the procedure.

Once the Applicant has read and agreed to the relevant terms and conditions, the procedure will continue.

5 Identification

You agree that (a) mesoneer or its Solution Partner will identify you in accordance with these Terms of Use and that audio and video recordings and still images will be made in the process; (b) mesoneer will forward the personal data that you have entered and that has been collected during the identification procedure and the identification documents to the Solution Partner for the purpose of verifying the authenticity of the identity documents. The data will remain in the EU and is subject to the EU General Data Protection Regulation (GDPR) and will be processed by mesoneer and its Solution Partner exclusively to carry out the identification procedure and subsequently transferred to the Partner for whom your identification is being performed. The privacy policies of mesoneer and its Solution Partner apply, and you will be informed of these as part of the procedure.

6 Terms of Use for Identification Verification

As the Applicant, you will use a technical device (e.g. your PC, tablet or smartphone) as part of the identification procedure to record a video of yourself and the identity document using the camera. The identification procedure is described below along with the steps involved and related data processing:

As an Applicant, you will usually be made aware of the identification service by the Partner of mesoneer. mesoneer usually requires end-user data such as, in particular, first and last name, date of birth, nationality, type of identity document and a mobile phone number to perform the identification service and, if applicable, to issue an electronic signature.

A photo and video of your identity document will also be taken as part of the identification procedure. Photos of the identity document and the Applicant's face are generated from the video recording and then compared with each other. In addition, data are extracted from the identity document in order to verify the identification.

As part of the identification procedure, data on the device, browser and internet access used (e.g. device type, operating system, IP address, access provider), data on the visit and page activities during the identification procedure (such as login with date/time, clicking an "Accept" button, etc.) are also collected.

The Applicant's data along with the video recordings and photos of the identity documents are stored by mesoneer and the Solution Partner only until they are transmitted to the Partner. Your data will be deleted from mesoneer's and the Solution Partner's servers after a period of 90 days at the latest if only an identification is performed without an electronic signature being issued. However, if the identification procedure is used as a basis for a electronic

certificate, in accordance with statutory requirements, the data must be retained and may not be deleted.

The Partner may also store the data for a longer period in order to comply with statutory archiving periods (e.g. within the scope of the Anti-Money Laundering Act). The handling of your data by the Partner as a data controller is governed by the Partner's respective privacy policies and your contractual relationship with the Partner. The provisions of the privacy policies of mesoneer and its Solution Partner apply in this regard.

7 Your Obligations

For your own security and to ensure that the identification procedure can be completed properly, you are required to observe the following basic rules.

(a) Use the procedure and identification in accordance with the terms and conditions set out in this document and the documents referenced therein (such as the CPS).

(b) Please note that the unlawful, indecent and/or potentially injurious use of the identification service is not permitted.

(c) You are obliged to enter up-to-date and correct data during the identification procedure and shall not provide false information or submit identity documents that have been falsified or tampered with in any way. In addition, the identity documents used must meet the following requirements:

- The identity documents used must bear a photograph and security features that can be verified automatically during video remote identification to ensure the detection of forgeries or tampering.
- The identity document is not a photocopy or a printed card.
- The identity document is not in a digital format (mobile phone, tablet or computer).
- The identity document is not in a cover.
- The identity document is not damaged, all information and security features are intact.

(d) The following points must be observed during the identification procedure and the video recording:

- The lighting in the video should enable a clear view of the face of the person to be identified and of the document.
- The video recording should be a constant stream with no interruptions or delays.
- The identification must be carried out "live".
- The identification will be rejected if someone other than the person to be identified guides them through the procedure.
- If another person is involved in making the video recording, but is clearly not forcing the person to be identified, the identification may be valid (e.g. if a person assists a physically or otherwise impaired person with the identification).
- All parts of the documents recorded (front and back) and the person's face must be clearly visible.
- The person to be identified must not be asleep or display signs of being under the influence of drugs or alcohol.

(e) When using the identification service, please follow the instructions and guidance provided by mesoneer or its Solution Partner.

Please note that you alone are responsible for the choice of data network that you use and for ensuring that your device is adequately protected against unauthorised access (see section 8 below).

8 Risks associated with the transmission of data on the internet and the general use of the Service

Please note that your data will be transmitted via the internet. You hereby acknowledge that there are risks associated with the transmission of data via such electronic means. mesoneer and the Partner do not assume any liability for the security of your data during transmission, nor for the proper functioning of the devices, systems and internet connections that you use.

Despite the use of state-of-the-art security technology, absolute security cannot be guaranteed on the part of the Partner, mesoneer and you as the

Applicant. While your device is a part of the overall system, it may become a weak point in the system since it is outside the Partner's and mesoneer's control. Despite all of the security measures that have been taken neither the Partner nor mesoneer can assume any responsibility for your device. You hereby acknowledge the following risks in particular:

a.) Inadequate knowledge of the systems and insufficient security features on the device can make it easier for others to gain unauthorised access (e.g. inadequately protected storage of data on the hard disk, file transfers, residual screen images, deletion of log-in data and means of identification from data storage devices).

b.) It is impossible to exclude the possibility of the Applicant's traffic being monitored by network operators (e.g. internet or text message service providers), this means the provider can track whom you have contacted and when.

c.) There is a risk that a third party may gain undetected access to the device while you are using the identification service.

d.) When using a network (e.g. the internet), there is a risk that viruses and similar may spread to your device when it is connected to external computer networks.

9 Intellectual Property

The elements and content that appear throughout the procedure, such as texts, photos, graphics, images, icons, technologies, software, links and other audiovisual or acoustic content, as well as the graphic design and source codes ("Content"), constitute the intellectual property of mesoneer and/or the Solution Partner. You are only granted the rights of use to the Content that you require in order to complete the identification procedure under these terms and conditions – no intellectual property is transferred. The trademarks, trade names or other distinctive marks of mesoneer, the Service Partner and/or third parties are also protected and reserved – your use of the Service does not confer on you any rights in the said trademarks, trade names and/or other distinctive marks.

10 Disclaimer

mesoneer and the Solution Partner guarantee that the Service as described in this document will be performed appropriately, provided that you fulfill the obligations imposed on you and also follow the instructions provided by mesoneer and/or the Solution Partner.

Access to and use of the Service and the video identification procedure in particular does not constitute any obligation on the part of mesoneer and/or the Solution Partner to check for viruses, Trojans and other malware. In any event, it is up to you, the Applicant to use appropriate tools to detect and eliminate malware. Neither mesoneer nor the Solution Partner shall be liable for any damage caused to the Applicant or third parties' ICT infrastructure while using the Service and conducting the video identification procedure.

The proper functioning of the Service and the identification in particular may depend on the correct configuration of the equipment you are using, and you are required, as set out, to follow the instructions provided during the identification procedure and to ensure compliance with the specified hardware and software requirements in all cases and at all times.

Similarly, you must ensure that you have internet access in order to use the Service. The proper functioning of the Service and the video identification procedure may depend, among other things, on the adequate quality and speed of the connection you choose in order to access the Service. Accordingly, you are responsible for ensuring the provision and sufficient quality of telecommunication lines, internet subscriptions or connections or other technical means yourself.

Neither mesoneer nor the Solution Partner shall be liable (a) for any damages arising out of or related to the non-performance or defective performance of your obligations under this Agreement; (b) the incorrect use of the results or output of the Service or passwords, or for any indirect damage that may arise out of the use of the Service or the information provided by mesoneer and/or the Solution Partner; (c) any inaccuracies in the identification of the Applicant arising out of information provided by the Applicant during the procedure; (d) for the correct functioning of third-party applications and services that are not authorised and for any damage caused by the fact that the Applicant is unable to use these applications.

11 Suspension of Use

If security risks are detected, mesoneer reserves the right to suspend the identification service at any time

until such risks have been resolved; this is both for your protection and for the protection of all users. mesoneer is also entitled to suspend your use of the service should you fail to comply with these Terms of Use. mesoneer accepts no liability for any loss or damage arising out of a suspension of the service.

12 Amendments to Terms of Use

mesoneer reserves the right to amend these Terms of Use at any time.

13 Severability Clause

The provisions of this document are independent of each other and, accordingly, if any provision is held to be invalid or unenforceable, the remaining provisions shall continue to be valid unless the Parties expressly agree otherwise. Ineffective or unenforceable provisions shall be modified in good faith so as to achieve to the greatest extent possible the purpose intended by the ineffective or unenforceable provision.

14 Applicable Law and Forum

This Services provided by mesoneer shall be governed exclusively by the laws of Switzerland with the exclusion of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods of April 11, 1980.

This Services provided by the Solution Partner shall be governed exclusively by the laws of Spain with the exclusion of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods of April 11, 1980.

Unless other mandatory consumer jurisdictions apply, the following exclusive jurisdictions shall have exclusive jurisdiction over any disputes arising out of or in connection with the Service: (a) for mesoneer services: the ordinary courts at its registered office (b) in respect of services performed by the Solution Partner: the ordinary courts in Madrid.

Personal Data Protection Information for the user

In fulfilment of the provisions of the current legislation on the protection of personal data and its implementing regulations, we are pleased to provide you with information regarding the processing of your personal data (hereinafter the "Data").

Data Controller: the data you provide us, now or in the future, for the purpose of our relationship, will be treated by eID as the Data Controller, whose registered office is located at Avenida Ciudad de Barcelona 81- A Planta 4ª, 28007, Madrid, with Tax Identification Code B86681533, and registered in the Madrid Company Registry. Registration Data: Volume: 30920, Book: 0, Folio: 146, Section: 8, Sheet: M556508 on April 3, 2013.

Legal Basis: the legal basis for the processing is the execution of the Contract to which you are a Party.

Purpose: as a Trusted Service Provider, your data will be processed by eID for the purpose of issuing and managing your electronic certificate as natural person, as well as to enable you to authenticate certain systems by means of an electronic signature; and to maintain, develop and control our relationship, which includes attending to your queries or requests for information or documentation.

All the data provided by the requester, through forms on the website or in the documents provided to the Registration and Identification Entities, as well as the Contracts signed with eID or with Registration and Identification Entities to issue certificates, will be used to issue the certificates and to manage them during their life cycle, and will be added to the certificate user database of which eID is responsible for, in accordance with the provisions laid down in the Service Contract and the Certification Practice Statement. By accepting this policy and the Certification Practice Statement, the requester consents to their personal data being processed for the purposes described.

In particular the purposes of the processing are: (i) to carry out the management, development, compliance and control of the contractual relationship; (ii) the sending of any type of postal or electronic correspondence related to this relationship; (iii) the inclusion of the data in the contact agendas of a corporate or departmental nature and of the employees who require it; (iv) the correct economic, accounting, tax and invoicing management derived from the legal relationship maintained; (v) management of the corresponding contractual file for the filing and maintenance of the history of contractual files; (vi) the issue of the electronic certificate of the natural person.

Data retention period: the Data will be kept for the term of the contractual relationship, until such time as deletion is requested, and during the period of limitation of any legal action that may be taken, or claims that may be received from official bodies, in relation to this Contract and after its termination. In any case, the maximum period of processing shall be 15 years from the time of issuance of the certificate, unless otherwise provided by law. Once our relationship is terminated, your Data will be duly blocked, in accordance with the provisions set forth in the applicable regulations.

Recipients: The Data will be communicated to the following recipients: (i) Judges, courts and law enforcement agencies, in compliance with legal requirements, obligations or in the framework of legal proceedings; (ii) banking institutions, for the management of collections and payments; (iii) tax authorities, for the fulfilment of tax obligations; (iv) financial auditors, for the fulfilment of financial obligations; (v) public authenticating officers in the event of the document being made public; and any other third parties to whom, in accordance with the applicable legislation in force in each case, the transfer is necessary, such as the competent administrative bodies, for reasons of control, registration and inspection.

The personal data of the users may be transferred and/or communicated to the members of the Community of Certificate Users when users use their electronic certificate or when they sign electronic documents whose verification involves the consultation of the data included in the file of users or certificate holder's responsibility eID.

In addition, the Data may be made available to third parties, both in Spain and in the European Union, for the purposes of the services they provide to our company (such as data hosting or identification support services), under a Processing Manager Contract, which guarantees the appropriate protection measures, in accordance with the provisions of the legislation on the Protection of Personal Data, and with the obligation of return and/or destruction at the end of the service.

International Transfers: There are no international transfers affecting the Data.

Rights: The data subject may exercise his or her rights of access, rectification, erasure, restriction of processing, opposition to processing, portability, and refusal to be the subject of automated individual decision making by sending a request to the following e-mail address: legal@electronicid.eu, or to the postal address: Avenida Ciudad de Barcelona 81- A Planta 4ª, 28007, Madrid; indicating the right he or she exercises and providing a photocopy on both sides of his or her ID card or legal identity identification document. The interested party is informed of the right to file a complaint in Spain with the Spanish Data Protection Agency (www.aepd.es) and to request information and protection from that body regarding the exercise of their rights.

You may revoke, by the means indicated above, and at any time, the particular consents we request from you in this clause, without retroactive effect and in the terms provided by law.

All the data that we request from you is obligatory, so any failure to comply with some of them may make it impossible for us to provide the services we offer. The electronic signature services offered by eID can only be performed if the requester provides all of the data requested truthfully and without including any false information.

The Data you provide us with must be correct and up to date at the time you provide us with the information, and you therefore guarantee its authenticity and truthfulness. In addition, we ask you to inform us of any changes to your Data, quickly and diligently, with the sole purpose of keeping our file permanently updated and without any type of error in relation to your Data.

Legal Age: Our services, as well as the goods that we provide in relation to e-trust through our platform can only be used by people of legal age. You hereby ensure that the information that you include regarding your date of birth is correct. The user will be sued for any liability that may be derived for eID caused by falsely indicating your age.

Confidentiality and security measures: We would like to inform you that eID will handle your data with the utmost confidentiality and as established in the uses and purposes expressly described above. We would also like to inform you that eID has implemented the technical and organizational measures necessary to guarantee the security of your data and prevent its unauthorized alteration, loss, processing, or access, taking into account the status of the technology, the kind of data being stored, and the risks it is exposed to, in accordance with the provisions in the applicable law on data protection.