/Terms and Conditions of the License to use the Solution of Veridas

In the event that VERIDAS and the End-Customer have entered into a separate license agreement covering the same Solution regulated in these T&C, the terms and conditions of such agreement shall prevail over any conflicting terms in these T&C. These T&C shall, however, remain in full force and effect for all matters not explicitly addressed or contradicted by the terms of the separate agreement.

This agreement describes the general Terms and Conditions (hereinafter, "**T&C**"), applicable to the use of the contents, products and services of Veridas Digital Authentication Solutions, S.L. (hereinafter, "**VERIDAS**") offered on the marketplace of Amazon Web Service (hereinafter, "**AWS**") to the End-Customer (you). Any individual or legal entity wishing to access or make use of Veridas technology may do so subject to these T&C by expressly accepting them on this platform.

PRIVATE OFFERS

VERIDAS will ONLY grant licenses through private offers.

- A private offer can be requested by clicking on the "Request private offer" button.
- If the CLIENT contracts our solution through a non-private offer (public offer), VERIDAS may cancel it and will not be obliged to provide the Service. If a payment has already been made by the CLIENT, VERIDAS will duly refund such amount. VERIDAS will not have any other obligation nor will be liable for any inconvenience or damage due to this situation.
- If the CLIENT contracts our solution through a non-private offer (public offer) and, exceptionally, VERIDAS at its sole discretion decides to accept it, VERIDAS will be able to propose changes to the accepted offer.

1. LICENSE GRANT AND SCOPE

1.1. By means of this license agreement (the "**License**"), VERIDAS grants in favor of the End-Customer a non-exclusive and non-transferable license over the use of VERIDAS' products including the Software (the "**Solution**"). The License is subject to the terms and conditions described in these T&C.

For the avoidance of doubt, it is stated that:

a) "**Software**" means the computer programs and documentation specified by VERIDAS, irrespective of the format in which they are contained. By way of non-exhaustive example, the Software may consist of source code and/or object code, SDKs, Docker containers, APIs, access to and use of the VERIDAS cloud, etc.
b) "**End-Customer**" means the legal entity that contracts the products of VERIDAS through AWS.
c) "**Offer**" is the commercial document(s) presented by VERIDAS to the End-Customer within the framework of this business or contractual relationship and previously accepted by the End-Customer within AWS, and which regulates, together with these T&C, the terms under which the services will be provided. Unless otherwise agreed at VERIDAS sole discretion, the Offer shall refer to "private offers" as explained above.
d) "**Parties**" refers to VERIDAS and the End-Customer.

Likewise, the license includes the technical support documentation for the use and operation of the Solution, including the user manual, the specifications and instructions for installation and use, as well as any additional information provided during the term of this agreement (hereinafter, the "**Documentation**"), the purpose of which is to ensure the correct functionality of the Solution and greater efficiency in its use and operation.

The license is granted to the End-Customer on a non-exclusive, non-assignable and non-transferable, non-commercial, indivisible basis, without the right to create derivative works, for the agreed duration and territory, for the purpose of providing the services described in the Offer.

1.2. The Solution may contain various components that may be subject to various applications. However, the license is granted for the whole of the Solution, and no separate use other than for the specific purpose agreed between VERIDAS and End-Customer. In this regard, unless otherwise previously authorized by VERIDAS in writing, the use of the SDKs may only be understood in connection with the use of the VERIDAS APIs and for such specific purposes.

1.3. For certain Solutions, if necessary, VERIDAS may install a computer application, in some cases connected with an external server (eventually with cloud connection), that allows VERIDAS to verify that the system is updated and payments are duly made. By accepting these T&C, the End-Customer acknowledges that it is aware of this requirement and expressly accepts it.

1.4. Upon termination of the License, regardless of whether it is due to the expiry of the term agreed or due to early termination under this contract or agreement of the Parties, the End-Customer shall stop using the Solution licensed by VERIDAS through AWS.

2. PERFORMANCE AND CONTINUITY WARRANTY

2.1. By accepting theseT&C, the End-Customer acknowledges that the Solution has an associated error rate which makes not possible, considering the state of the art, to guarantee a complete level of reliability. On the other hand, the outputs of the system are not binary but they offer a probabilistic result that has to be configured by the End-Customer depending on its requirements.

VERIDAS informs the End-Customer and the End-Customer accepts that it is its responsibility to carry out any necessary internal control evaluation, to implement due diligence measures in accordance with the regulation the End-Customer has to comply with (including without limitation: regulation on the prevention of money laundering, citizen security, border controls, gambling access control, underage and whitelists access control, etc.), as well as assessing the suitability of using the Solution as a tool to comply with the legislation in force in each case.

VERIDAS will provide information on the error levels and error rates of each version of the Solution. Additionally, it must take into account the functionalities that are covered by VERIDAS' Software for each platform. These levels of reliability are closely related to the conditions under which the evidence is captured in the process, so VERIDAS is not responsible for any use that the End-Customer may make of the Solution under conditions other than those recommended by VERIDAS.

VERIDAS provides some tools that may help the End-Customer to implement prevention mechanisms, being the End-Customer the solely responsible for the study of the convenience of its implementation, the specific configuration of the Solution, or the use made of it (expressly including the validation results obtained with the Solution), or the sanctions imposed by the competent authorities concerning the alleged breach of the due diligence measures.

2.2. As a protective measure, VERIDAS applies capacity limits to each end-customer to prevent excessive costs resulting from DDoS attacks, looped processes or similar on the client side. These limits are set automatically, at values above the observed End-Customer's consumption in the last few days of production. In the event that the End-Customer knew or could anticipate a sudden (extraordinary) increase in processes consumption (e.g. a marketing campaign), the End-Customer must inform VERIDAS at least two (2) business days in advance through support ticket, so that VERIDAS can scale the End-Customer's capacity. Otherwise, the service could be limited in response to the abnormal traffic received.

3. TERMS OF USE

3.1. The License granted under this agreement authorizes the End-Customer to use the Solution, including the right to its installation, presentation, execution, transmission and storage, when applicable, for the indicated

duration and for the provision of the services agreed in the Offer, always in accordance with these T&C and other applicable agreements signed with VERIDAS.

3.2. The obligations assumed by the End-Customer with respect to the use of the Solution include, notwithstanding any other obligations as specified in this agreement, in subsequent agreements signed between AWS and the End-Customer, or in applicable regulation:

i) The End-Customer may not use the Solution for any purpose other than those permitted previously and in writing by VERIDAS.

ii) The End-Customer may permit its employees to use the Solution for the agreed purposes, provided that the End-Customer takes all necessary steps and imposes the necessary conditions to ensure that all employees using the Solution do it within the agreed purposes and that they do not commercialize or disclose the contents of it to any third party, or use it other than in accordance with the terms herein.

iii) The End-Customer will not distribute, sell, license or sub-license, lease, trade or expose for sale the Solution to a third party, unless expressly agreed in writing with VERIDAS.

iv) No copies of the Solution are to be made.

v) No changes to the Solution or its content may be made.

vi) The End-Customer will provide technological and security measures to ensure that the Solution, which the End-Customer is responsible for, is physically and electronically secure from unauthorized use or access.

vii) The End-Customer shall ensure that the Solution retains all VERIDAS copyright notices and other proprietary legends and all trademarks or services marks of VERIDAS.

viii) The End-Customer shall not, under any circumstances, use reverse engineering practices on the Solution.

ix) The resolution of errors and mistakes derived from the system integration carried out by the End-Customer or its suppliers, and not offered by VERIDAS, will be the sole responsibility of the End-Customer.

x) The End-Customer may evaluate the performance of the service after its integration within its systems doing a penetration test. The conditions of such penetration test shall be agreed by the Parties in advance. VERIDAS strongly recommends this measure.

3.3. VERIDAS may supervise compliance with the conditions of use in the event of suspicion of fraudulent use.

3.4. In accordance with AWS requirements, VERIDAS may share with AWS information about the End-Customer's use of the Solution through AWS (usage data). To this extent, no personal data of end users is intended to be shared unless expressly agreed and regulated with the End-Customer.

4. LIABILITY

4.1. Within the limits established by law, the End-Customer knows and accepts the technological limitations of the Solution, which are described in Clause 2.1, and exonerates VERIDAS, its directors, employees and agents from any responsibility derived or related to any claim, loss or damage arising as a result of the supply by VERIDAS of the Solution, or derived from any use of the Solution by the End-Customer or its employees, insofar as it does not arise from an act or omission by VERIDAS according to the provisions in these T&C.

4.2. Notwithstanding the application of the previous general clauses and other provisions that may be established in this agreement or in the Documentation, VERIDAS expressly excludes the following situations, as well as any damages that may arise from them, from its scope of responsibility:

i) willful, fraudulent, deliberately unlawful acts, penalized as a criminal offense, or which are voluntarily against the law, carried out by or against the End-Customer or its employees;

ii) willful, fraudulent, deliberately unlawful acts, penalized as a criminal offense, or which are voluntarily against the law, carried out by third parties (either individuals or legal entities) through or making use of AWS' and/or End-Customer's systems that incorporate the Solution, especially in view of the provisions of Clause 2.1 of these T&C;

iii) any fact or circumstance, real or suspected, the End-Customer knows about or could have reasonably foreseen, and that may affect, in any way, to the correct functionality of the Solution, provided it is not due to a serious act or omission of VERIDAS;

iv) mechanical failures, electric failures (including interruptions, outages, overvoltages or power curst) and failures on telecommunication or satellite transmission systems, provided that those failures are not due to an act or omission of VERIDAS or to an error of the delivered Solution;

v) any issue related to the software services, content (including code) found at third-party websites or third-party programs given that those issues are not due to an act or omission of VERIDAS or to an error of the delivered Solution;

vi) damage or loss of the End-Customer´s data resulting from the failure of VERIDAS and/or AWS' systems to store or preserve such data, as well as the costs resulting from such circumstance, unless such preservation is a service contracted for under the Offer;

vii) any act or claim alleging, derived from or based on funds, money or value transfers or any other negotiable instrument for or from a bank or financial institution;

viii) failure to comply with its obligations and warranties due to force majeure or fortuitous event; or

VERIDAS will not be liable under or in connection with these T&C or any Offer (whether in contract, tort or otherwise) for any special, indirect or consequential losses, including loss of profit, loss of anticipated savings, loss of business opportunity, loss of or corruption of data or loss of reputation or goodwill; suffered or incurred by the other party (whether or not such losses were within the contemplation of the Parties at the date of these T&C and/or the Offer). VERIDAS will not be liable for loss suffered by the CLIENT to the extent VERIDAS cannot independently substantiate and/or respond to a claim due to the fact that the CLIENT has instructed VERIDAS to delete the underlying information.

4.3. Regarding the obligations of the End-Customer as data controller (according to Annex I of these T&C), the End-Customer must inform data subjects regarding the processing of their personal data and, if applicable, obtain their consent, complying with the applicable regulations on data protection and privacy. The End-Customer shall indemnify, defend and hold harmless End-Customer against any claim filed by data subjects, especially for this cause. The above shall also apply to claims and responsibilities demanded by the data protection authorities and other competent authorities or courts in relation to the obligations of the data controller. In the event that the End-Customer is the data processor (being its client the data controller), the End-Customer will be responsible for transferring the above responsibility to its client.

4.4. In any case, where permitted by the legislation in force, the liability of VERIDAS shall be limited, in the totality of the claims, to the amount invoiced during the last twelve (12) months in relation to the customers and/or Solutions concerned. The foregoing limitation shall not apply, and the setting of the amount indicated shall be determined by the final judgment or decision of the competent authority in the matter, in the case of:

i) breaches of data protection, confidentiality, intellectual and industrial property, fiscal, tax, labour, social security or anti-corruption regulations;
ii) loss or damage caused by wilful misconduct or gross negligence;
iii) personal injury or death; or
iv) where unlimited liability is mandatory by law.

5. TECHNICAL SUPPORT AND ASSISTANCE

5.1. VERIDAS will provide the End-Customer with a support service on the Solutions in accordance with the terms and conditions agreed in the Offer and, if any, in the Documentation. VERIDAS shall not be liable for defects or errors caused by the intervention of a technical support that has not been previously authorized in writing by VERIDAS.

5.2. If the End-Customer requires additional support, it may be quoted and invoiced separately. Unless otherwise provided in such eventual new support offer, the clauses of these T&C shall apply to the support services.

5.3. VERIDAS will communicate to the End-Customer the way in which incidents and/or support requests should be reported so that they can be analyzed by VERIDAS, and VERIDAS will determine if they are covered by this service. In order for VERIDAS to provide technical support in the terms indicated, the End-Customer must first provide an explanation to the problem encountered so that VERIDAS can understand how the problem occurred, which could be done through screenshots and as much information as reasonably possible.

6. SERVICE LEVEL AGREEMENT (SLA)

6.1. Included is the use of APIs located in the VERIDAS cloud, which is hosted on AWS servers within the European Union and/or the United States, depending on the region selected by the CLIENT (if other regions are required, VERIDAS is open to discussion).

6.2. VERIDAS undertakes to make reasonable efforts in order to provide its services in the production cloud environments with an availability annual ratio of at least 99.5%, unless otherwise expressly agreed in writing.

6.3. The previously mentioned percentage shall not apply to any unavailability, suspension or expiration of the service, or any other interruption of the service that:

i) results from a suspension or termination of the agreement;

ii) is caused by external factors beyond VERIDAS' control, including any force majeure or Internet access events, and any related problems;

iii) results from voluntary or involuntary omissions or actions of AWS, the End-Customer or a third party;

iv) results from AWS' or End-Customer's systems, software or any other technology, or any other software or technology from a third party;

v) resulting from maintenance windows and emergency maintenance; or

vi) affects the monitoring portal.

6.4. If the maintenance activities mentioned in Clause 6.3.(v) affect the availability of the service, the hours during which such maintenance activity is performed shall be: for cloud-enabled services in Europe between 00:00 am and 07:00 am, and for services that make use of the cloud in the USA between 06.00 am and 01.00 pm (Madrid, GMT +2 CEST).

7. PRICE AND METHOD OF PAYMENT

7.1. The Price to be paid for the License will be determined by the Offer accepted by the End-Customer.

7.2. The Price will be paid to VERIDAS through AWS in the terms agreed in the Offer and in the agreements signed between VERIDAS and AWS. In no case shall VERIDAS be affected by delays or defaults in payment terms between AWS and the End-Customer.

8. DATA PROTECTION

8.1. In relation to the processing of personal data derived from the use of the Solution, the End-Customer acknowledge and accept that VERIDAS is not responsible for the data collected by the use of the Solution within the activities of the End-Customer, not it is the controller of such data in terms of the General Data Protection Regulation (GDPR) and other applicable legislation.

The End-Customer recognizes that VERIDAS needs to access the personal data collected by the Solution as data processor (or, eventually, data sub-processor). This processing will be carried out based on the data processing agreement included in Appendix I of these T&C.

8.2. During the integration and testing activities, the End-Customer may make use of VERIDAS' APIs endpoints in a test environment or sandbox (usually identified as "apis-work"), in order to perform the integration of the Solutions in their systems. Using this environment does not exempt the End-Customer from its duty of care and good diligence in accordance with data protection regulations.

Where applicable, VERIDAS' access to the personal data collected by the Solution in this sandbox environment will also be done in its condition as data processor (or, eventually, data sub-processor). This processing will be carried out based on the data processing agreement included in Appendix I of these T&C.

9. INTELLECTUAL PROPERTY RIGHTS

9.1. The Parties declare to hold the ownership of their intellectual property rights (IPR) and/or the necessary authorizations, for the uses required by these T&C, in accordance with the applicable legislation. In the event of a claim by a third party for infringement of IPR, each Party shall be responsible for the corresponding infringement, exonerating the other Party from any responsibility in this regard.

9.2. Each Party shall retain title to its IPR held prior to the commencement of the relationship. The signing of these T&C shall in no way imply the assignment, transfer, acquisition or licensing of IPRs.

9.3. All IPRs on and relating to the Solutions are the property of VERIDAS and/or its suppliers. The End-Customer does not acquire by contracting the services and obtaining the license any right over the property of the Solution/s or any other intellectual asset or IPR, and may only make use of the IPRs of which it has an explicit and unequivocal permission, in the manner specified by VERIDAS in these T&C and associated with the agreed purpose.

9.4. Any adaptation, modification or improvement made to the Solution, and the know-how related to such process, shall be the sole property of VERIDAS and/or its suppliers.

10. CONFIDENTIALITY

10.1. "**Confidential Information**" shall mean any information or material owned by either Party, regardless of whether the Party is its owner and/or creator or not, which is not generally known by third parties beyond the organization itself and its employees, and to which the other Party may obtain access, directly or indirectly. Without prejudice to its specific identification as confidential or private, it must be understood that the Confidential Information includes any information provided by the Parties in relation to the business, technology and information of the Party and/or third parties with which the Party has, including, but not limited to, reports and business plans, trade secrets, technical information, product ideas, contracts, financial information, pricing structure, discounts, computer programs, source and/or object codes, intellectual and industrial property rights, inventions, customers and potential customers, strategic alliances, partners and collaborators. The nature of the information and the manner in which it is disclosed must be such that the Party understands that it is Confidential Information.

10.2. The Parties agree to use the Confidential Information of the other Party as reserved and protected, to use it exclusively for the purpose and compliance of these T&C, and to no disclosure, reproduce or make it available to third parties without the previous written consent of the Party.

10.3. The obligations of confidentiality set out immediately above shall not be applied to any Information which: a) the receiving Party is required to disclose it under law, binding court orders or by any governmental authority (by oral questions, interrogatories, requests for information or documents, subpoena, civil or criminal investigative demand or similar process); b) the receiving Party was authorized, in writing, to disclose, but exclusively within the limits and conditions set for such disclosure; c) it was previously in possession of the receiving Party without a confidential requirement; d) is or becomes publicly available through no act or omission of the receiving Party; or e) is disclosed to the Party by a third party who to the receiving Party's best knowledge was entitled to disclose it to it and which the receiving Party is not required to maintain in confidence.

10.4. In the event that a Party knows that it is going to be, or it is probable that it will be, required to disclose Confidential Information under law, binding court orders or by any governmental authority, this Party should, to the extent permitted by law, promptly (and, in any event, before complying with any such mandatory requirement) notice the other Party of such requirement so that it may seek a protective order or other appropriate remedy.

10.5. Each Party undertakes to assure that the Confidential Information received from the other Party is treated with at least the same degree of protection and confidentiality as it safeguards its own Confidential Information, but in no event with less than due care. Each Party shall restrict access to the Confidential Information to only those of its employees, representatives, consultants or advisors to whom such access is necessary or appropriate for the Party to carry out the Services, and provided they have agreed on confidentiality obligations equivalent to those established herein.

10.6. Notwithstanding any other provisions of this Agreement, the Parties hereby acknowledge that a breach by any Party of the provisions in relation to the non-disclosure of Confidential Information will cause the Parties irreparable damage and the Parties shall be entitled to seek timely injunctive relief to protect its rights.

10.7. The confidentiality and no-disclosure obligations set in this Clause will continue in force after the expiration of this Agreement.

10.8. Notwithstanding the above, the Parties hereby allow each other to inform third parties of the existence of a contractual relationship between the Parties, and may use their trademark, commercial name and logo for this specific purpose. For this purpose, in no case shall any Confidential Information be disclosed.

11. TERMINATION

11.1. Without prejudice to the duration of the Offer or to the validity and enforceability of those clauses and conditions that should subsist upon the termination of the T&C (as provided for herein, its own nature or as provided for by law), the breach of any of the obligations set forth in these T&C by any of the Parties and not remedied in accordance with Clause 11.2 below, shall entitle the other aggrieved Party to choose between the termination of the Agreement, or to demand its compliance.

11.2. In particular, the Parties may terminate the T&C before the end of the term in the event of any of the following causes:

a) in the event that one of the Parties fails to comply with any of the terms of these T&C and does not remedy it in a manner satisfactory to the other Party within fifteen (15) days from the date of notification;

b) in the event that one of the Parties fails to comply with Clause 9 or Clause 10 of these T&C, and does not cure the same in a manner satisfactory to the other Party immediately (and at the most within three (3) days) after notification thereof; or

c) in the event that one of the Parties becomes insolvent, initiates (or is commenced against) bankruptcy, insolvency, reorganization or dissolution proceedings, or makes any assignment in favor of any creditor.

11.3. In any event, the foregoing general provisions shall be without prejudice to the right of the aggrieved Party to request compensation for the data and damages that the non-performing Party may have caused it, under the conditions established in Clause 4 of these T&C.

12. MISCELLANEOUS

12.1. AMENDMENT AND WAIVER. No variation of these T&C or any Offer will be valid unless it is agreed in writing and signed by both of the Parties. Failure or delay in exercising any right or remedy under these T&C or any Order Form will not constitute a waiver of such (or any other) right or remedy.

12.2. SEVERABILITY. If any provision of these T&C or Offer (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision will, to the extent required, be deemed not to form part of the T&C or Offer as applicable and (a) the Parties will immediately commence good faith negotiations to remedy such invalidity; and (b) the validity and enforceability of the other provisions of the T&C or Offer as applicable will not be affected.

12.3. ENTIRE AGREEMENT. These T&C and the applicable Offer constitute the whole agreement between the Parties and supersedes any previous arrangement, understanding or agreement between them relating to the subject matter of this Agreement and the applicable Offer. **This shall be understood without prejudice of the disclaimer included at the beginning of these T&C regarding previous license agreements applicable to the same Solutions.**

12.4. NO ASSIGNMENT. Neither Party may assign any of its rights or obligations under these T&C without the prior written consent of the other.

12.5. ACT OF GOD. Neither Party will be liable for any delay or non-performance of its obligations under these T&C or any Offer to the extent that such delay or non-performance is a result of any condition beyond its reasonable control (a "**Force Majeure Event**"). To the extent that a Force Majeure Event occurs, End-Customer

acknowledges that VERIDAS may be required (and will be permitted) to change the manner in which it provides the services.

12.6. SUBLICENSES. The End-Customer shall not sublicense VERIDAS' Solution unless expressly authorized by VERIDAS. In such a case, the End-Customer will be responsible for transferring to the sublicensed entity the same terms and conditions established in these T&C. In the event that the agreed sub-license implies the introduction of a functionality or country different from those initially foreseen in the Offer, the End-Customer recognizes that a new development may be necessary by VERIDAS and, therefore, could imply additional costs over which the Parties will have to negotiate.

12.7. EXECUTION. These T&C shall be deemed known and accepted by both parties upon acceptance through the AWS platform by the End-Customer. Both parties acknowledge that these T&C have not been unilaterally imposed by either party, and that there has been sufficient opportunity for discussion, negotiation, and mutual agreement prior to acceptance.

12.8. GOVERNING LAW AND JURISDICTION. These T&C will be construed by and governed in accordance with the Laws of Spain. All disputes over this Agreement shall be definitively resolved by means of arbitration administered by the Spanish Court of Arbitration in accordance with its Regulations and Statutes, entrusted with the administration of the arbitration and the nomination of the arbitrator or arbitrators.

Appendix I

Personal data processing agreement (DPA)

1. Purpose of the processing assignment

By these clauses, the End-Customer authorises VERIDAS to process personal data on its behalf. In this regard, VERIDAS acts as "**Data Processor**" and the End-Customer as "**Data Controller**".

The processing of personal data is inherent to the Service described in the T&C, including the correct operation of the different components of the Solution, where applicable, as well as the anonymisation or pseudonymisation of certain data aimed, where applicable, at verifying the operation of the same, without prejudice to other processing agreed in writing between the Parties.

The specific processing is described in more detail in the table contained in Clause 6 of this Appendix ("**1. Processing Description**").

2. Identification of the affected information

For the execution of the services derived from the fulfilment of the object of this processing commission, and in accordance with the applicable legal provisions, the Data Controller makes available to the Data Processor the personal data necessary for the provision of the services described in this agreement.

The table contained in Clause 6 of this Appendix ("**2. Processed Data"**) includes specific personal data to be processed.

3. Duration

The contents of this Appendix shall be valid for the duration stated in the T&C.

In this respect, the retention period for personal data shall be as detailed in the table in Clause 6 of this Appendix ("**3. Retention periods**").

4. Obligations of VERIDAS as Data Processor

The Data Processor and its entire staff undertake to:

a. Use the personal data processed, or any data collected to be added, for the purpose of the assignment only. Under no circumstances may the data be used for the Data Processor's purposes.

b. Process the data as per the instructions issued by the Data Controller.

   Where the Data Processor considers that any of the instructions breaches the GDPR or any other provision on data protection from the EU or its Member States, the Data Processor will inform the Data Controller thereof immediately.

c. Keep a written record of all categories of processing activity carried out on behalf of the Data Controller; this record must contain the following:

   1. The name and contact details of the processor(s) and each controller on behalf of which the Data Processor acts and, where appropriate, the details of the controller's or processor's representative and the data protection officer.
   2. The categories of processing carried out on behalf of each controller.
   3. Where appropriate, transfers of personal data to a third country or international organization, including the identification of said country/organization and, for the transfers mentioned in the second paragraph of article 49(1) of the GDPR, the documentation for appropriate safeguards.
   4. A general description of the technical and organizational security measures regarding:
      i. Pseudonymization and encryption of personal data.
      ii. The capacity to guarantee the permanent confidentiality, integrity, availability and resilience of the processing systems and services.
      iii. The capacity to restore the availability and access to personal data quickly, in the event of a physical or technical issue.
      iv. The process for regularly checking, assessing and evaluating the efficacy of the technical and organizational measures in view of guaranteeing secure processing.

d. Not disclose the data to third parties or transfer them to third countries or international organizations unless the Data Controller's express authorization has been obtained, as per the legally admissible conditions.

   The Data Processor may disclose the data to other data processors working for the same Data Controller, as per the instructions issued by the latter. In this case, the Data Controller will provide prior written identification of the entity to which the data must be notified, which data are to be disclosed and the security measures to apply in this eventuality.

e. Subcontracting

   The provisions in the Agreement and in the Offer will govern the subcontracting by the Data Processor of other service provision companies that must process personal data from the Data Controller.

   In this regard, the specific sub-processors are detailed in Appendix I ("**4. Sub-processors**").

   Any change in the subcontracted entities will be notified by the Data Processor to the Data Controller, through the usual channels, and the Data Controller will have a period of five (5) working days to communicate any objection to the Data Processor.

   When subcontracting, the Data Processor shall ensure that an agreement with the sub-processor has been entered into with guarantees equivalent to those contained herein. If the subcontracting implies an international transfer of personal data, the Parties will previously agree, in writing, the terms that shall apply to such subcontracting.

f. Uphold the duty of secrecy as it refers to the personal data it may have access to under this assignment, even after the end of its purpose.

g. Guarantee that any individuals authorized to process personal data expressly undertake, in written form, to respect their confidentiality and to observe the relevant security measures, of which they must be duly informed.

h. Place the documentation certifying its compliance with the obligation above at the disposal of the Data Controller.

i. Guarantee that the individuals authorized to process personal data receive the necessary training in personal data protection.

j. Assist the Data Controller with responding to the exercise of the following rights:

   1. Access, rectification, erasure and objection.

2. Limitation of processing.
3. Data portability.
4. Not to be object of individual automated decisions, including profiling.

When the data subjects exercise their rights of access, rectification, erasure and objection, limitation of processing, data portability and to not be the object of individual automated decisions with the Data Processor, the latter must report the situation via email to the address provided by the Data Controller. This notice must be sent immediately and never later than the next business day after the request is received; the email must also include, where appropriate, any other relevant information to fulfill the request.

k. Right to information

The Data Controller must facilitate the right to information when the data are collected.

l. Notification of data security breaches

The Data Processor will immediately –without undue delay– inform the Data Controller if the former becomes aware of breaches of the personal data under its responsibility, providing all relevant information for documenting and notifying the incident. This information must immediately be sent to the address provided by the Data Controller.

It is not necessary to send this notification when it is unlikely that the data breach will pose a risk to the rights and freedoms of natural persons.

If available, the following information will be provided at a minimum:

1. Description of the nature of the data breach including, when possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected personal data records.
2. The name and contact details of the data protection officer or any other point of contact from which more information may be obtained.
3. Description of the possible consequences of the data breach.
4. Description of the adopted or proposed measures for resolving the data breach including, where applicable, the measures adopted to mitigate possible negative effects.

If the information cannot be provided simultaneously, and to the extent that this is not possible, it will be supplied gradually and without undue delay.

The Data Controller will be responsible for notifying security breaches to the data subjects when the breach is likely to pose a high risk to the rights and freedoms of individuals.

m. Support the Data Controller in performing impact assessments regarding data protection, where applicable.

n. Support the Data Controller in submitting prior queries to the control authority, where appropriate.

o. Provide the Data Controller with all the information needed to demonstrate the fulfillment of its obligations and to facilitate auditing or inspections by the Data Controller or an auditor authorized by the Data Controller.

p. Implement the following security measures:

The Data Processor must comply with the provisions of the legislation in force regarding the personal data processed during the provision of Services under the Agreement. Additionally, the Data Processor must respect the agreements made with the Data Controller as regards the purposes of processing.

Specifically, the Data Processor must comply with the applicable obligations stipulated in the GDPR and the Spanish regulation on data protection.

At all events, the mechanisms to achieve the following must be implemented:

1. Guarantee the permanent confidentiality, integrity, availability and resilience of the processing systems and services.
2. Restore the availability and access to personal data quickly, in the event of a physical or technical issue.
3. Regularly check, assess and evaluate the efficacy of the existing technical and organizational measures in view of guaranteeing secure processing.
4. Pseudonymize and encrypt personal data, where appropriate.

q. Appoint a data protection officer and inform the Data Controller of their contact details.

In this sense, the Data Processor informs that a data protection officer has been appointed and can be reached at dpo@veridas.com.

r. Destination of data:
   - Delete the personal data and any copies within the timelines described in Appendix I ("**3. Retention Periods**"). This includes complete deletion of the existing data from the IT equipment used by the processor.
   - However, the Data Processor may retain a copy, with the data blocked, while it is still liable for executing the service provision.

5. Obligations of End-Customer as Data Controller

The Data Controller must:

a. Provide the Data Processor with the data mentioned in section 2 of this DPA.
b. Assess the impact on personal data protection of the processing operations that will be performed by the Data Processor.
c. Make prior consultations as applicable.
d. Ensure that the Data Processor complies with the GDPR before and during processing.
e. Oversee processing, including inspections and audits.
f. Comply with the obligations that the GDPR establishes for the Data Controller, without prejudice to others so established in the T&C, License and/or DPA.
g. With regard to the process of informing the data subject and obtaining the relevant consent, the Data Controller undertakes to ensure and guarantee that the user does not make use of the Solution without having been previously informed and having given consent. For the avoidance of doubt, this responsibility is not transferred to the Data Processor.

6. Processing specialities

	Digital Identity Authentication and Verification Solutions
1. Processing Description	Collection, communication, recording, deletion. a) Processing carried out in Productive environments: The Data Controller is responsible for capturing the user's data and sending it to the Data Processor's APIs located on cloud servers (AWS). The Data Processor analyzes the received data, proceeding, as applicable to the contracted services, with the validation and extraction of data from the identifying document, with facial biometric comparison, with the completion of a life proof, etc. After these tasks have been completed, the Data Processor returns the received data to the Data Controller, along with the results of all checks performed, and this information is not stored on VERIDAS servers. Additionally, the Data Processor will perform the processing of personal data for the purpose of active fraud monitoring. Specifically, VERIDAS may detect and perform a forensic analysis of processes suspected of being fraudulent, according to the results obtained during the validation process and, if applicable, would actively report them to the Data Controller, all with the aim of being able to provide the Data Controller with in-depth information on the operation of its processes incorporating the VERIDAS Solution, and to be able to improve and robuster the services offered by VERIDAS for which purposes it may anonymize such data. The period of storage of personal data by the Data Processor for the purpose of active fraud monitoring shall be 60 days. b) Processing carried out in non-productive environments (sandbox): The Data Processor provides the Data Controller with a test and integration environment (sandbox) for use with fictitious data or internal data from the Data Controller that can be used for these purposes (i.e., not real end-user data). This environment is intended for the Data Controller to perform tests, check the functioning of the Solution, verify correct integration with its own systems, etc. These environments also serve for joint work between the Data Controller and the Data Processor's support teams, so that

	incidents or defects detected can be analyzed and monitored, the system can be adapted and improved, especially in the face of new use cases or particularities, help with the correct integration of the Solution and its subsequent versions, etc.
2. Processed Data	• Identification data. • Biometric data for identification purposes.
3. Retention periods	a) Regarding personal data processed in production environments: Unless otherwise agreed by the Parties, the Data Processor will delete the personal data once data is sent to the devices and/or systems of the Data Controller (no copies are made). For personal data that for any reason are not sent and/or deleted by the Data Controller, the Data Processor will implement a periodic automatic cleanup process, which will remove all validations with an age greater than one (1) hour. This time is subject to modification if agreed by the Parties. If the storage of personal data is included in the Services contracted from VERIDAS, it will be retained for the duration of the Contract unless otherwise specifically agreed between the Parties. At the end of this period, VERIDAS will return and/or delete the personal data (as agreed) without applying a blocking period. b) Regarding personal data processed in non-production environments (sandbox): The Data Processor will delete the personal data within a maximum of five (5) years or the maximum set by applicable legislation in case it is lower. Notwithstanding the foregoing, at any time after the testing or sandbox period, the Data Controller may request that the Data Processor delete such personal data.
4. Sub-processors	Amazon Web Services, as IaaS and PaaS provider, located in the European Economic Area and in the United States of America, depending on the region selected by the CLIENT. Both regions are separated and personal information will not be shared between regions unless previously required by the CLIENT.
5. Specific Obligations of the CLIENT as Data Controller	[Applicable in the event that data storage by VERIDAS is included in the contracted Services] When VERIDAS is required to store personal data, the Data Controller must indicate the data retention periods that apply in each case.