DATA PROCESSING AGREEMENT

FOR IVSIGN, IVCERT, IVNEOS & VIDEOID

The purpose of this Data Processing Agreement (DPA) Annex is to comply with the provisions of Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, the General Data Protection Regulation or GDPR) and by virtue of the provisions of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter, 'LOPDGDD') of Spain, the processing of personal data on behalf of third parties requires the conclusion of a private contract establishing the purpose, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, as well as the obligations and rights of the controller.

This DPA is presented as an Annex to the General Terms and Conditions of Contract generated with the Purchase Order, and therefore its express acceptance occurs jointly with the signing of the aforementioned Purchase Order and attached documentation.

This Data Processor Agreement consists of the following

CLAUSES

FIRST. - DEFINITIONS - ROLES OF THE PARTIES

The concepts presented throughout the following contract, such as personal data, processing, data controller, data processor, pseudonymisation, encryption, etc., shall be understood as defined in accordance with the GDPR and the LOPDGDD and the data protection authorities.

CLIENT: the Party that contracts the Services from the PROVIDER and that will generally act as the 'Controller of personal data' (the 'CONTROLLER'). In cases where the CLIENT is a Partner (authorised distributor or collaborator), the latter shall be considered the PROCESSOR, the PROVIDER as the SUB-PROCESSOR and its customers as CONTROLLERS (and so on if there are more parties involved). Hereinafter, we shall refer exclusively to the CONTROLLER, without prejudice to the fact that the CLIENT may be a Partner.

PROVIDER: a Signaturit Group company that provides Services to the CLIENT and end users, which will generally act as the Data Processor (the "PROCESSOR").

SUPPLIER: is the legal entity belonging to the Signaturit Group that provides the Services to the CLIENT and therefore maintains the main contractual relationship with the CLIENT (or Prime Contractor).

- The SUPPLIER shall act as the PROCESSOR if it is also the PROVIDER that will provide the final service to the CLIENT and users.
- If the CLIENT has contracted services provided by another SERVICE PROVIDER belonging to the Signaturit Group through the SUPPLIER, the SUPPLIER shall not be involved in the processing of personal data relating to the provision of the service.

SECOND. - PURPOSE

2.1. Purpose of the contract

The purpose of this contract is to establish the terms and conditions that will govern the processing by the PROCESSOR (and, where applicable, the SUB-PROCESSOR) of the personal data contained in the CONTROLLER's systems, for the purpose of providing any of the processing services covered by the Service Provision Contract signed between both parties for the purpose and in accordance with their instructions

and the GDPR. Hereinafter, we will refer exclusively to the PROCESSOR, without prejudice to the fact that the SUPPLIER may be considered a SUB-PROCESSOR.

2.2. Data processing carried out

The following table details the processing activities to be carried out on behalf of the CLIENT, according to the content of the service provision contract signed between the parties:

SERVICES	IVSIGN	IVCERT	IVNEOS	VIDEOID
Description	Certificate centralisation and remote signature service	Electronic evidence management service for electronic document signing and certified electronic delivery processes (email and SMS communications)	Electronic notification management service	Remote video identification and OCR service
Data Subjetcs	A. Application users B. Digital certificate holders	A. Application users B. Digital certificate holders C. Recipients of electronic signature and communication processes.	A. Application users B. Digital certificate holders C. Third parties (notified)	A. Users of the application. B. Holders of identity documents.
Types of data	A. User identification: name, surname, email, tax identification number or equivalent, department, position, organisation. B. User contact details: email address, telephone number. C. Those included in certificates: name, surname, tax identification number, email, organisation, position and others (of the application user or third parties). D. User service usage and audit log: IP, URL, application and equipment where the certificate is used, date of operation.	A. User identification: name, surname, email, tax identification number or equivalent, department, position, organisation. B. User contact details: email, telephone number. C. Those included in the certificates: name, surname, tax identification number, email, organisation, position and others (of the application user or third parties). D. User service usage and audit log: IP, URL, date of operation. E. The contents of the documents sent by the platform. Freely chosen by the Data Controller. F. The contents of the evidence according to the functionality used in the application: *Biometric signature data. Image data from identity documents used by OCR.*	A. CUSTOMER identification and contact details: name, surname, email address, tax identification number or equivalent. B. User identification and contact details: name, surname, email address. C. Identification and contact details of third parties (e.g. customers, collaborators, suppliers of the CUSTOMER): name, surname, email, postal address, tax identification number or equivalent, NAF. D. Those included in the certificates: name, surname, tax identification number, email, organisation, position and others (of the application user or third parties). E. Regarding the user's use of the service and audit log: IP address. F. Metadata associated with notifications: with personal data of the application user or third parties	A. User identification: name, surname, email address, tax identification number or equivalent, department, position, organisation. B. User contact details: email address, telephone number. C. Those included in identification documents: name, surname(s), tax identification number. D. User service usage and audit log: IP address, URL, date of operation. E. Proof of life and identity: Image data from identity documents used by OCR, video.
Processing	A. Collection, storage, retention and deletion of the types of data indicated B. Queries made by the user and by administrator users C. Export of data (lists) by the user and by administrator users D. Recording and consultation of usage activity (reports and audits) E. Preparation of lists and reports for service management by the Provider F. Sending of notices and communications related to the provision of the service G. Cross-checking of personal data (Video ID only).			

Purposes	Managing remote electronic signatures for any user purpose (access to premises, signing documents, VPNs, etc.)	Collecting electronic evidence of operations carried out with documents and communications sent through the application.	Managing electronic notifications sent to electronic headquarters for any purpose of the user. Communicating with public administration websites.	Verify the authenticity of identification documents, establish onboarding mechanisms through OCR and proof of life.
Retention periods	In the case of qualified trust services, the retention period for data issued and received by the provider is 15 years from the end of the service provided (Art. 9.3-a) Law 6/2020).	• Documents and data issued and received by the provider in the qualified electronic delivery service: - Qualified: 15 years from the end of the service provided (Art. 9.3-a) Law 6/2020). - Non-qualified: 2 years • Documents subject to transactions and data issued and received by the Provider in the electronic signature service (evidence): configurable time for each responsible customer (by default, 2 years accessible from the platform + 3 years in secondary storage accessible on demand).	There is no applicable retention period as the customer downloads the notifications to their computers.	• For the purpose of issuing certificates, will keep the video recording, photos, identity document scans and automatic result (Order ETD/495/2021): - 15 years if the process is OK from the expiry of the certificate - 5 years if the process is rejected from the date of execution. • For other purposes: customisable for each responsible client (12 months applies by default)

2.3. Obligations and measures

The aforementioned processing will be carried out in accordance with the provisions of the GDPR, the LOPDGDD and any other applicable data protection regulations.

Likewise, the PROCESSOR shall process the data of the natural persons signing this contract, those existing between the parties and those of the natural persons who are workers or users of its services for the purpose of managing this contractual relationship entered into between the Parties consisting of the provision of trust services. This personal data will be kept for the time necessary to fulfil the purposes for which it was collected, provided that the signatories do not revoke the consent given. Subsequently, if necessary, the information will be kept blocked for the legally established periods, after which the information will be finally deleted.

THIRD. - DUTY OF CONFIDENTIALITY AND PROFESSIONAL CONFIDENTIALITY

3.1. Professional confidentiality

The PROCESSOR shall maintain professional confidentiality in relation to all personal data of the CONTROLLER to which it has access as a result of the provision of services established in the Contract.

3.2. Duty of confidentiality

All personnel under the responsibility of the CONTROLLER who access and/or process personal data are subject to professional confidentiality and confidentiality obligations, which shall remain in force even after the provision of services has ended.

In this regard, only those employees of the PROCESSOR who need to access personal data in order to carry out their duties for the provision of services may access such data.

The PROCESSOR shall inform its employees of the obligations contained in this contract and the confidential nature of the information they process, while requiring them to comply with those obligations that may be applicable to them in accordance with the applicable regulations, and shall warn them of the liability they would incur in the event of disclosure.

Furthermore, whether employees perform the contracted services on the CONTROLLER's premises or remotely, the CONTROLLER shall duly inform them of the rules and procedures to which they are subject, as well as any other provisions they must observe in accordance with the instructions provided by the CONTROLLER's staff.

3.3. Breach of these duties and consequences

Any breach by the PROCESSOR or its staff of the duty of confidentiality regarding the aforementioned data or any other obligation arising from personal data protection legislation shall be grounds for termination of the main contract and, as a consequence, of this contract.

FOURTH. - COMPLIANCE WITH INSTRUCTIONS BY THE PROCESSOR

4.1. General obligation – Data communications

The PROCESSOR may take all organisational and operational decisions necessary for the provision of the contracted service. However, the decisions taken must in all cases comply with the instructions given by the CONTROLLER.

Notwithstanding the foregoing, for the purpose of complying with the provisions of the service provision framework, data communications may occur between the companies of the Signaturit Group for administrative and support functions and all those necessary for the proper provision of the service. You can consult the composition of the Signaturit Group at https://www.signaturit.com/legal-notice/

4.2. Specific obligations

The obligations are, among others, descriptive in nature, but not limited to, the following:

1. Security obligations

   The SUPPLIER (and, where applicable, the final service provider) has an information security management system (ISMS) in place, implementing best practices for information security management in accordance with the UNE-ISO/IEC 27001 standard, the National Security Scheme and the ISO/IEC 22301 standard, applying to all data processing carried out within the framework of the contracts formalised with the CLIENT the controls and measures aimed at guaranteeing the security of the personal data for which the CLIENT is responsible and to which it has access as a result of the contract.

   Furthermore, the SUPPLIER declares and guarantees that it will carry out the necessary periodic checks and security audits to verify that the security controls and measures implemented are effective for the treatment of the risks for which they have been implemented in each case.

2. Not to apply or use the personal data to which it has access in the performance of the functions entrusted to it for purposes other than those established in this Contract, and not to communicate such data, even for the purposes of storage, to third parties, unless otherwise provided by law or court order.

3. The PROCESSOR is obliged to keep the personal data provided by the CONTROLLER under its control and custody, and not to disclose or transfer it, even for storage purposes, with the exception of the provisions of clause Six of this contract.

4. In any case, access to and processing of the data by the Data Controller shall be subject to the security measures adopted to comply with the principle of proactive responsibility enshrined in Article 5.2 of the GDPR.

5. The Data Processor's staff must expressly undertake to respect confidentiality and to comply with the security measures corresponding to the processing of the CONTROLLER's data.

6. Keep a written record of all categories of processing activities carried out on behalf of the CONTROLLER, containing:
    a. The name and contact details of the processor or processors and of each controller on whose behalf the processor acts and, where applicable, of the representative of the controller or processor and of the data protection officer.
    b. The categories of processing carried out by the Processor.
    c. Where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in Article 49(1), second paragraph, of the GDPR, documentation of appropriate safeguards.
    d. Keep a record of the security measures applicable to its systems, in this case based on the ISO/IEC 27001 information security standards and the National Security Scheme.
7. Not to subcontract any of the services that form part of the subject matter of this Contract that involve the processing of personal data derived from the provisions of this Contract or the main contract, with the exception, however, of the auxiliary services necessary for the normal functioning of the CONTRACTOR's services, which are listed in Annex I.
    a. For the hiring of Sub-processors by the PROCESSOR, the CONTROLLER must be notified in writing at least thirty (30) days in advance, indicating the processing operations to be subcontracted and clearly and unambiguously identifying the subcontractor and its contact details. The CONTROLLER shall be deemed to have consented to the subcontracting if it does not expressly refuse in writing to the PROCESSOR within thirty (30) days of the notification.
    b. Once the subcontracting has been authorised, the PROCESSOR shall sign a data processing agreement with the sub-processor, the content of which must comply with current data protection regulations and the security and confidentiality obligations set out in this data processing agreement.
    c. In the event of non-compliance by the sub-processor, the initial PROCESSOR shall remain fully liable to the CONTROLLER with regard to compliance with the obligations.
8. Notify the CONTROLLER, without undue delay, of any security breaches affecting personal data owned by the CONTROLLER that you become aware of in any case within twenty-four (24) hours, by email and in a reliable manner.
    a. The notification must contain all information considered relevant for the documentation and communication of the incident. Specifically, and provided that it is available, the following must be provided:
        i. Description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
        ii. The name and contact details of the data protection officer or other contact point where further information can be obtained.
        iii. Description of the possible consequences of the personal data breach.

iv. Description of the measures taken or proposed to address the personal data breach, including, where appropriate, measures taken to mitigate any possible adverse effects.

b. If it is not possible to provide the information simultaneously, and to the extent that it is not, the information shall be provided gradually without undue delay.

9. Support the data controller in:

   a. Carrying out data protection impact assessments, where applicable.

   b. Carrying out prior consultations with the supervisory authority, where appropriate.

10. Providing data subjects, in collaboration with the CONTROLLER, with the information necessary to comply with the information obligation under Articles 13 and 14 of the GDPR and Article 11 of the LOPDGDD. The wording and format in which the information is provided must be agreed with the CONTROLLER before data collection begins.

11. Allow the CONTROLLER to carry out audits, either in interview or documentary format through the preparation of questionnaires, with the aim of verifying the proper fulfilment of the obligations of the PROCESSOR, based on the provisions of this Contract. In any case, the Parties declare that the CONTROLLER:

    a. must give the PROCESSOR at least thirty (30) days' notice and may not exceed one audit per year, unless the PROCESSOR reports a security breach with a serious impact on personal data or there has been a sanction by a data protection authority against the PROCESSOR;

    b. shall be responsible for the entire cost of the audit (including any costs, expenses and fees associated with it) and its duration shall not exceed two full working days, regardless of the format chosen by the CONTROLLER, nor shall it require the assigned person to devote more than the aforementioned two days to it. If the time and resources required exceed those indicated, the SUPPLIER shall notify the CLIENT in advance so that the CLIENT can adapt the scope of the audit to reduce it to the effort included or agree to bear the SUPPLIER's costs. The frequency of these audits shall be annual.

    c. They shall not disrupt the normal activity of the CONTROLLER. In any case, the dates and deadlines for carrying out the audit may be adapted by the CONTROLLER depending on the availability of the personnel assigned to carry them out.

    d. in the event of proposing documentary audits consisting of the completion of documentation or forms, the deadline for completion shall not be less than thirty (30) days, and this deadline may be adjusted if required by the SUPPLIER.

FIFTH. - SECURITY MEASURES TO BE IMPLEMENTED BY THE PROCESSOR

The PROCESSOR may have or shall have access to computer and documentary media owned by the CONTROLLER, such as data relating to potential or end customers of the CLIENT, as well as employees or other types of users (hereinafter referred to as "Users"). Therefore, the PROCESSOR, in its capacity as Processor, undertakes to apply the following security measures:

1. Specific definition of the processing carried out. The PROCESSOR provides the services detailed in the framework contract, for which it may access the personal data of data subjects for whom the CONTROLLER is the Data Controller or Data Processor, as applicable, in accordance with current regulations. The table in section 2.2.1 Processing Activities to be carried out for the contracted Services indicates the processing activity for the contracted service.

2. Type of access. The PROCESSOR has access to the CONTROLLER's computerised or documentary data for the purpose of providing the services detailed in the main contract.
3. Place of processing. Processing by the PROCESSOR will be carried out electronically, by sending reports, lists and reports on the aforementioned users to the CONTROLLER's systems, among others, when requested.
4. Security measures applied: The PROCESSOR has the following security measures in place:
   a. *It has a system for assigning usernames and passwords to its employees, both for its own systems and for third-party systems, whereby access is limited according to user profiles, through the assignment of personalised usernames and passwords that expire at least once a year.*
   b. *It has informed its staff of their rights and duties regarding the processing of third-party data, with express reference to the personal data provided by customers.*
   c. *It has an up-to-date list of user profiles and permissions, both for its own systems and those of third parties.*
   d. *It has an incident reporting system in place, as well as a protocol to follow in the event of an incident, both internally and in relation to the CONTROLLER, users or supervisory body.*
   e. *It shall take appropriate measures for the transfer of media, whether its own or that of third parties, if applicable.*
   f. *It has an up-to-date inventory of assets.*
   g. *It has a system for making daily backups of its computer systems.*
   h. *It has a Business Continuity Plan and a Disaster Recovery Plan that forms part of a Business Continuity Management System audited and certified to the UNE ISO 22301 standard.*
   i. *A Data Protection Officer has been appointed and can be contacted at the following address:* dpo@signaturit.com
   j. *Data protection audits have been or are being carried out every two years.*
   k. *It has a system for recording the entry and exit of media that may contain sensitive personal data, which complies with the parameters of the law.*
   l. *Unauthorised access to its computer systems is restricted, as it has secure areas with limited physical and logical access.*
   m. *In its incident reporting and recording system, it is also permitted to record the data recovery process, in accordance with the parameters of the applicable regulations.*
   n. *It fully applies the security measures established in its Information Security Management System, which is audited and certified under the ISO 27001 standard and under the National Security Scheme.*

SIXTH.- ASSISTANCE IN COMPLIANCE WITH THE RIGHTS OF DATA SUBJECTS

The PROCESSOR shall assist the CONTROLLER in responding to the exercise of the rights of:

- Access, rectification, erasure and objection
- Restriction of processing
- Data portability
- Not to be subject to automated individual decision-making (including profiling)

To this end, when data subjects exercise their rights of access, rectification, erasure and objection, restriction of processing, data portability and not to be subject to automated individual decision-making before the data processor, the latter must notify the data controller by email to the address indicated, providing the details of the parties involved.

The communication must be made immediately and in no case later than the working day following receipt of the request, together with, where appropriate, other information that may be relevant to resolving the request.

SEVENTH. - COMMITMENTS AND OBLIGATIONS OF THE CONTROLLER

The CONTROLLER declares that it complies with all the technical and organisational measures necessary to guarantee the security of the processing, data processing centres, premises, equipment, systems, programmes and persons involved in the processing of the personal data referred to.

The CONTROLLER is responsible for the guarantees of the data subjects, such as the rights of access, rectification, erasure and restriction of processing.

When using the Services, the CONTROLLER must comply with applicable legislation. Consequently, all instructions from the CONTROLLER regarding the Processing of Personal Data must comply with Data Protection Legislation and the CONTROLLER is solely responsible for the accuracy, quality and legitimacy of such personal data and the means by which it has been obtained.

The CONTROLLER undertakes to notify the PROCESSOR of any changes to the personal data provided, so that the latter can update it.

EIGHTH. - DURATION AND TERMINATION OF THE CONTRACT

This Contract is considered ancillary to the provision of services specified in the main Contract, and therefore its duration and termination are subject to said link or main contract.

Upon termination of the contract, the PROCESSOR shall return the personal data and, where applicable, the media on which they are stored, to the data controller once the service has been provided, unless it is appropriate or possible to destroy them, in which case this shall be done after notifying the CONTROLLER and certifying afterwards that this has been done.

In any case, the return must involve the total erasure of the data existing on the computer equipment used by the processor. However, the PROCESSOR may keep a copy, with the data duly blocked, for as long as liabilities may arise from the performance of the service, in order to comply with the PROCESSOR's legal commitments, always in accordance with the principles of confidentiality and data minimisation.

NINTH.- APPLICABLE LEGISLATION AND JURISDICTION

This Contract shall be governed by the clauses contained herein and, in matters not provided for therein, by the applicable Spanish and European regulations on the processing of personal data.

Any disputes relating to the interpretation or application of this contract shall be subject to the provisions agreed by the Parties in the Service Provision Contract or General Terms and Conditions of Contract.