nebulaSUITE®

General Conditions of Service

V.3.6.4 | November 2025

vintegris

Index

FIRST: Definitions

Service-Level Agreement: Clauses or particularities of the contract signed between the parties or included in these General Conditions that develop and stipulate the services objectively in terms of level and quality that will be applicable.

Third-party applications / third-party software: Third-party applications that may interact with VÍNTEGRIS software.

Client: Natural or legal person, duly represented, who contracts the nebulaSUITE Services provided by VÍNTEGRIS. The Client declares unless otherwise agreed, that he owns the equipment on which the application is used or is authorized to use them. Likewise, it states that it has sufficient powers to bind the legal entity it represents to bind it to the VÍNTEGRIS documentation and these General Conditions so that the use and payment of these services will be sufficient proof of the perfection of the contracts and to act with sufficient representation to bind the company it represents.

Partner: A company that meets the requirements to participate as a reseller of VÍNTEGRIS solutions, who acts on its behalf, with its organization and in direct relationship with the Clients who consume VÍNTEGRIS solutions and services.

General Conditions: Refers to these general conditions, applicable in all cases to the Service, and its annexes.

Particular Conditions: Refers to the particular conditions that stipulate, where applicable, the personalized details of the Service and the auxiliary services agreed between VÍNTEGRIS and the Client**.**

Client Data: Those Data entered by the Client that will be systematically collected and accessible individually by VÍNTEGRIS.

Equipment: Computers, tablets, smartphones, and any other electronic machines capable of storing information and processing it for the correct development of the software or equipment that interacts with the VÍNTEGRIS service.

License: Rights granted by VÍNTEGRIS to the Client in the terms and conditions included in the relevant contract and which include, among others, the limits to copy, install, use, display and run the software.

Complementary Program: It is any tool or software component that belongs to or is licensed by VÍNTEGRIS and that VÍNTEGRIS makes available for download as part of the Cloud Services to facilitate Your access, operation and/or use of the Services Environment. Does not include Third-Party Technology licensed separately.

Economic proposal: This includes the specifications of the service contracted by the Client, including the number of users who can access the contracted Services.

SaaS Service: Software as a Service (Software as a Service). These are services provided over the Internet by VÍNTEGRIS in favor of the Client concerning the use of the contracted service through the SaaS Services platform and within the cloud computing infrastructure.

Applicant: Natural person who, for the purposes of these General Conditions, acts in the name and representation of the Client and who REQUESTS VÍNTEGRIS to provide the nebulaSUITE service.

User: Person authorized by the Client to use the VÍNTEGRIS Software.

VÍNTEGRIS: It is the company VÍNTEGRIS, SLU, with address at Calle Pallars 99, floor 3, office 33, 08018 Barcelona, Spain, and CIF B-62913926, and registered in the Mercantile Registry of Barcelona.

SECOND: VÍNTEGRIS Services

The Applicant, a natural person who, for the purposes of these General Conditions, acts in the name and representation of the Client, REQUESTS VÍNTEGRIS to provide the nebulaSUITE service. nebulaSUITE includes the following services:

Name of Service	Description
nebulaUSERS	User management service
nebulaID	Video Identification service
nebulaCERT	Centralised certificate management service
nebulaACCESS	Dynamic multifactor authentication service
nebulaSIGN	Digital Signature service
nebulaSNE	Electronic notification management service
nebulaDISCOVER	Digital certificate discovery service

The indicated services are provided by VÍNTEGRIS in SaaS mode after their selection by the Client or licensee, using various computer applications owned by VÍNTEGRIS located on a technological platform to which the Client will have access once the relevant use licenses have been granted.

THIRD: Mandatory nature of the General Conditions

These General Conditions for Contracting Services ("General Conditions"), without prejudice to the documents listed in Clause Six, regulate the use of all nebulaSUITE services.

The "General Conditions" applicable in each case for each Client correspond to the latest version that the Client accepts and signs at the time of the initial contract/renewal of the subscription to the service. Failing that, the General Conditions published on the website, in force at the time of contracting/renewal, will apply.

This version of the "General Conditions" will be applicable and valid during the contracted or renewed subscription period (12 months by default).

Each year the subscription is renewed, VÍNTEGRIS reserves the right to modify, periodically and at its sole discretion, the General Conditions, these new updated conditions being applicable in the next renewal of the Client's subscription, taking into account what is indicated in the previous paragraph and with the exception of the indications described in clause eighteen.

The Client accepts and undertakes to make correct use of the nebulaSUITE services in accordance with all applicable laws of the European Union and Spain, as well as with the corresponding regulations, rules, notices, criteria, reports and technical standards that result, originating (collectively called "Laws"), and in accordance with the rules of good faith, public order and contained in the General Conditions, without prejudice to the order of priority established in the Twenty-sixth clause.

These General Conditions are implemented subject to the Laws, their agreements, and the declaration of trust practices (DPC) in force at the time of the provision of each service, and which can be found updated at the internet address https: //www.vincasign.net/

FOURTH: Hiring process

To contract the Service, the Applicant must sign the acceptance sheet included in the economic proposal, which declares acceptance of the Specific Conditions and General Conditions attached to the economic proposal.

Once the corresponding documentation is signed, VÍNTEGRIS will give the Client access to the Platform.

The conclusion of the contracting process is subject to verification of the data provided by VÍNTEGRIS. Once the contract has been completed, VÍNTEGRIS will send the Client a Purchase Confirmation Letter by email that will contain the subscription contract data. Furthermore, except in the case of renewals, VÍNTEGRIS will send the Client by email a document called "Welcome Info (WI)", which will include the instructions for accessing the platform, the validity period of the subscription, the User for access and the Client's email address where the link to reset their password will be sent to them.

It should be noted that the start and end dates of the subscription (validity period) will be those indicated in the “Welcome Info (WI)” document. The start date will coincide with the environment activation date and the date from which The subscription is contracted until the end date, which is the maximum contracted date. These dates will be the ones that will be taken as a reference to take into account the expiration of the subscription and its renewal.

The password established by the email is unique, personal and non-transferable. It will be the Customer's obligation to make diligent use of and keep their passwords or other credentials secret. Consequently, the Client is responsible for the adequate custody and confidentiality of any identifiers and/or passwords and undertakes not to transfer their use to third parties, whether temporary or permanent, or to allow their access to outsiders. The Client will be responsible for using the Services by any illegitimate third party who uses a password for this purpose due to non-diligent use or loss of the password by the User. By virtue of the foregoing, it is the Client's obligation to immediately notify VÍNTEGRIS of any fact that allows the improper use of identifiers and/or passwords, such as theft, loss, or unauthorized access to them, in order to proceed to its immediate cancellation. As long as such facts are not communicated, VÍNTEGRIS will be exempt from any liability arising from unauthorized third parties' improper use of identifiers or passwords.

It is advisable to modify this password periodically and not use the same password for several services.

FIFTH: Limitations of the applicant

The Applicant, at the time of requesting the nebulaSUITE services and in accordance with current legislation, has been informed of the precise instructions for the use of the services, the limitations of use and the way in which VÍNTEGRIS limits its possible liability, as well as the sufficient authorization of VÍNTEGRIS, and the relevant dispute resolution procedures, and accepts them expressly and without any reservation, for the purposes of what is indicated in articles 5 and 7 of Law 7/1998, of April 13, on general contracting conditions.

SIXTH: Regulation of nebulaSUITE services

The nebulaSUITE services are specifically regulated by the following service documentation, which is fully incorporated into the contract: 1º) Economic Proposal and the Particular Conditions that it incorporates. 2º) These General Conditions. 3º) Annex I "Specific Terms of nebulaSUITE Services". 4º) Annex II "Service-Level Agreements (SLA)". 5º) Annex III "DPA, Data Processing Agreement."

SEVENTH: Rates, billing and payment method

The Client will pay the amount corresponding to the services referred to in these General Conditions in accordance with the list of rates approved by VÍNTEGRIS at all times and whose current value is indicated in the Economic Proposal approved by both parties prior to the start of the contract provision of nebulaSUITE services. Without prejudice to what may appear in the list of rates, the price that the Client must pay is the one that appears in the Economic Proposal.

The prices of the services contracted by the Client are found in the Economic Proposal, as well as the details of the services and technologies contracted by the Client.

In the event that the Client contracts the services through a VÍNTEGRIS partner, VÍNTEGRIS will invoice the Partner for the corresponding amount indicated in the Financial Proposal approved by both parties prior to the start of the provision of the nebulaSUITE services.

The Partner will pay the corresponding amount according to the payment conditions established in the Financial Proposal.

In these cases, VÍNTEGRIS will not be responsible for the commitments that the Partner has acquired directly with the Client; it will only respond according to the services agreed and contracted by the Partner for the Client.

VÍNTEGRIS reserves the right to increase the prices of subscriptions to its products, which may be due, inter alia, to cost increases to compensate for new added functionalities, costs of new procedures and certifications imposed by regulations or to the expansion of new services added to the subscriptions. If VÍNTEGRIS foresees such an increase, VÍNTEGRIS will notify the customer 60 days in advance of the renewal date of the affected subscriptions and the customer may decide whether to renew or terminate their subscriptions.

The payment method and billing milestones are included in the Financial Proposal.

All payments will be made in euros (€) unless otherwise indicated in the Financial Proposal.

VÍNTEGRIS will invoice the Client according to the following:

a. **Standard Billing**

    1. 100% of the Technology and Services will be invoiced (these up to 5 days) after being made available to the Client (activation of the environment / sending of "Welcome Info")

b. **Special Billing.** After making it available to the Client, the milestones and billing amounts are as follows:

    1. 100% of the Technology (activation of the environment / sending of "Welcome Info").
    2. 50% of the Services at the beginning of the project. The remaining 50% upon completion after the Client's approval (when greater than 5 days).

In the event that the Client contracts the services through a VÍNTEGRIS Partner, the policies related to billing and payment indicated above will apply directly to the Partner.

If the Client does not pay all or part of the amounts owed after a period of one month has elapsed from the agreed invoice due date, VÍNTEGRIS may, upon prior notice to the Client, temporarily suspend the service. The restriction of the service will affect the services with respect to whose payment there has been arrears, and may affect other dependent services. The temporary suspension does not exempt the Client from the obligation to continue paying the corresponding fixed periodic instalments.

VÍNTEGRIS may also suspend or cancel the provision of the Service in the event that:

(a) The Client fails to comply with any of the obligations under his responsibility in accordance with these General Conditions or the Specific Conditions applicable in his case;
(b) has provided false or incorrect information in the application for registration in the Service;

(c) VÍNTEGRIS considers and/or has reasonable indications that illicit, illegal activities could be carried out through the Service, contrary to public order and/or good customs or contrary to what is stipulated in the General Conditions themselves.

Delay in payment for a period greater than 2 months or temporary suspension of the contract on two occasions due to late payment of any of the contracted services will entitle VÍNTEGRIS to the definitive interruption of all contracted services and the corresponding resolution. of the contract, after notifying the Client 10 business days in advance, indicating the date on which it will take place.

The policies relating to the suspension and cancellation of services due to non-payment will also apply in cases where their contracting has been carried out through VÍNTEGRIS partners, and both billing and payment have been delegated to them, and He did not pay his payment.

The Partner may request VÍNTEGRIS to deactivate each active Subscription separately, and depending on the Solution, the Client will have limited or no access to the Solution. VÍNTEGRIS will not be responsible in any way to the Client for the deactivation of the Client's Subscription by the Partner.

EIGHTH: Validity

Except for clauses 9, 10, 11, 12 and 19, the validity of these General Conditions will correspond to the service provided and will appear in the WI document or, failing that, in the purchase confirmation. The remaining clauses will remain in force as long as the legally established deadlines in each case do not expire or, if not established, as long as the legal actions that VÍNTEGRIS may exercise against the Client or third parties do not prescribe or expire.

NINTH: Termination of services

The Services under this Contract will be provided during the Service Period defined in the WI document or, failing that, in the purchase confirmation, unless suspended or early terminated in accordance with these General Conditions or the Economic Proposal.

Early termination without justified cause. Customer may choose to cancel their subscription early at any time, but will not receive a refund of previously paid fees and will be required to immediately pay all unpaid fees due through the end of the Subscription Term. In this case, the service will remain active until the initially defined expiration date, with the exception that the Client expressly tells us to deactivate the account.

Early termination for a justified cause. Either party may terminate the provision of the Services for cause as follows: (i) upon thirty (30) days notice to the other party that a material breach has occurred, provided that such breach has not been resolved at the end of the period. In this case,

VÍNTEGRIS reserves the right to access the service, the SaaS Service will be immediately deactivated for the Client, and the license to use the software related to the Services will terminate; all of this without prejudice to any right of access in relation to personal data, as provided in clause 17 of these General Conditions.

Also, VÍNTEGRIS may terminate the provision of the Services for cause with thirty (30) days' notice if VÍNTEGRIS determines that the Client is acting (or has acted) in a manner that reflects negatively on VÍNTEGRIS or affects VÍNTEGRIS or its prospects or clients.

In any of the aforementioned cases, if it is VÍNTEGRIS that declares the termination of the services due to infringement or improper action on the part of the Client, the Client will not receive any refund of previously paid fees and must immediately pay all unpaid fees owed until the end of the Subscription term.

Except for these reasons, the Service may not be terminated prior to the end of the Subscription Term.

Termination within the subscription period. In the event that the Client wishes to non-renew the subscription service, the Client must notify it at least one month in advance of the current subscription date. Otherwise, the Client may be required to pay cancellation charges and the rest of the conditions specified in this cancellation section.

If you cancel the Services, they will terminate on the end date of the current Service period or, if VÍNTEGRIS charges invoices to your account periodically, at the end of the period in which you made the cancellation.

To cancel the Services, you must contact your Commercial manager or communicate it to the address customercare@vintegris.com.

Please note that you will be obligated to pay all charges made to your billing account for the Services by the date your subscription ends.

TENTH: Software use license

Unless accompanied by a separate license agreement between VÍNTEGRIS and Customer, any software provided to you by VÍNTEGRIS as part of the Services is subject to these Terms:

(a) A temporary, onerous, non-exclusive, non-transferable license is granted in accordance with the provisions of these General Conditions and, where applicable, the Specific Conditions for the right of reproduction for the purposes of the right of use in relation to the nebulaSUITE service modality. Contracted in exchange for payment of the fee established in Clause 7.

(b) The software or website that is part of the Services may include third-party code. Any script or code belonging to third parties, linked to or referenced from the software or website, is licensed to you by the third-party owners of such code and not by VÍNTEGRIS. Any notices contained herein regarding third-party code are for informational purposes only.

(c) VÍNTEGRIS reserves all rights in the software that VÍNTEGRIS does not expressly grant under these Terms. This license does not grant any rights with respect to the following. Specifically, the licensee cannot do the following if it is not authorized, in writing, by VÍNTEGRIS:

i. Circumvent or bypass any technical protection measures contained in or related to the software or Services;
ii. Disassemble, decompile, decrypt, emulate, exploit a vulnerability or reverse engineer all or any part of the software or any other aspect of the Services included in or accessible through them, without prior written permission from VÍNTEGRIS , except and only to the extent such activity is expressly permitted by applicable Intellectual Property Law;
iii. Copy, modify, create derivative works, or otherwise attempt to extract the source code of the Software or any of the VÍNTEGRIS Services;
iv. Sublicense, transfer, reproduce or distribute any of the Services;
v. Sell, resell or otherwise make the Services and/or Software available to a third party as part of a commercial offer that has no material value independent of the Services;
vi. Reproduce, distribute, sell, transform, publish, publicly communicate, rent, lease or transmit to any person or entity, in whole or in part, in any form or by any means, whether mechanical, magnetic, photocopy or any other , without prior written permission of VÍNTEGRIS, the software.
vii. Separate components of the software or Services for use on different devices;
viii. Publish, copy, rent, lease, sell, export, import, distribute or lend the software or Services;
ix. Transfer any software, software licenses or rights to access or use the Services;
x. Use the Services in an unauthorized manner that may interfere with any other person's use of or access to services, data, accounts or networks or in any manner inconsistent with applicable Law;
xi. Allow access to the Services or modification of devices authorized by VÍNTEGRIS by unauthorized third-party applications;

xii. Create telematic "links" with the services described in this Agreement, nor adapt or duplicate any content of the Software on any other server or wireless device;
xiii. Access the product or services that are the subject of these General Conditions in order to create a competitive product or service or create a product using ideas, features, functions or graphics similar to those of the services provided therein.

Access to the Service is only allowed to those people who have the password, under the responsibility of the Client, and the Service will be limited to the corresponding number of users according to the Services contracted by the Client and in accordance with what is described in the Economic Proposal.

ELEVENTH: Guarantee

Saas services are made up of elements of different contractual causes, on the one hand, that derived from the software license and, on the other, that derived from its deployment in cloud infrastructure.

1.- **Regarding defective compliance derived from the VÍNTEGRIS software:**

VÍNTEGRIS guarantees that: (i) it will provide the Services in all material aspects as described in these Conditions and the Specific Conditions; (ii) will professionally provide the Services in accordance with these Conditions and the Specific Conditions; and (iii) you will not knowingly introduce any viruses or other forms of malicious code into the Service.

To the extent permitted by law, VÍNTEGRIS Services are provided "as is" without any warranty or condition in addition to that set forth in the preceding paragraph.

If the Services provided to the Client were not provided in accordance with the previous guarantee, the Client must notify VÍNTEGRIS in writing of this, describing the deficiency in the Services.

In the first 5 days, a diagnosis will be made by VÍNTEGRIS of the technical reasons for defective compliance in the provision of its services in accordance with these General Conditions and the Particular Conditions.

In the event that the restoration of the service could be done in less than 10 days, VÍNTEGRIS will make all commercially reasonable efforts to correct the situation and will propose alternative technical measures to the Client to minimize the possible damages that could affect the Client.

If it is not possible to provide the services in accordance with the previous guarantee within 15 days from the notification of defective performance. In that case, VÍNTEGRIS will propose alternative technical measures to the Client to minimize possible damages that could affect the Client. Within sixty (60) days from the date of notice of breach, either party may terminate the Services by sending written notice to the other.

The return of prepaid amounts from the moment of breach of warranty will be VÍNTEGRIS' RESPONSIBILITY, converting said amount into the maximum compensation for damages that the Client can claim and demand from VÍNTEGRIS, provided that it is not attributable to gross negligence or fraud. of VÍNTEGRIS.

2.- **Regarding defective compliance derived from the availability of the cloud infrastructure.**

In this sense, Annex II is an inseparable part of this contract, where the terms of the Service-Level Agreements (SLA) that VÍNTEGRIS offers to its Clients are developed.

TWELFTH: Limitation of liability and exclusion of guarantees

Any liability on the part of VÍNTEGRIS for non-compliance with the service level as established in ANNEX II will only be granted if VÍNTEGRIS is responsible for the non-compliance.

In particular, VÍNTEGRIS is **not** responsible for:

(a) No unavailability, suspension or termination of any of the services, or any other problem in their performance: (i) resulting from a suspension; (ii) caused by factors beyond the reasonable control of VÍNTEGRIS, including any force majeure event or Internet access or related problems beyond its point of demarcation; (iii) resulting from any action or omission on the part of the Client or a third party; (iv) resulting from Client personnel, software or any other technology and/or equipment, software or technology of a third party (other than third-party equipment that is under the direct control of VÍNTEGRIS); (v) resulting from a suspension and termination of the Customer's right to use the services in accordance with the service contract; (vi) that affects test, development, pre-production environments or environments for commercial purposes; (vii) that results from your failure to follow VÍNTEGRIS instructions; or (viii) that resulting from your equipment, software or other technology and/or third-party equipment, software or other technology (other than third-party equipment that is under the direct control of VÍNTEGRIS.

(b) The modification of the VÍNTEGRIS service by any other person or the modification by VÍNTEGRIS of said service in accordance with the specifications or instructions provided by the Client.

(c) The contents include links to third-party websites and activities provided by users. Such content and activities are not attributable to VÍNTEGRIS, nor do they represent the opinion of VÍNTEGRIS.
(d) Compensate for any damage, direct or indirect that is a consequence of using the service in a way that violates the Law or these General Conditions.
(e) Non-compliance or delay in the performance of its obligations under these General Conditions to the extent that such non-compliance or delay arises from circumstances beyond the reasonable control of VÍNTEGRIS (for example, labor disputes, natural phenomena, wars or terrorist activities, malicious damage, accidents, or compliance with applicable legislation or government regulation). VÍNTEGRIS will work to minimize the effects of such events and fulfil its obligations that are not affected by them.
(f) The unavailability, suspension or termination of any of the contracted services or any other performance problem as a result of the preventive and corrective maintenance carried out by VÍNTEGRIS in accordance with the "Evolution of the service" section described in Annex II, as long as this is communicated to advance to the Client.

VÍNTEGRIS will only be liable if the material obligations of the Contract are intentionally breached or when required by applicable law.

Additionally, unless agreed in writing, VÍNTEGRIS will not be obliged to make any modification to its systems or services to adapt them to operational requirements demanded by any regulatory or business need of the Client.

Neither party will be liable for any indirect, incidental, special, punitive or consequential damages or for any loss of profits, revenue (excluding fees due under this Agreement), data or data use.

The total liability of VÍNTEGRIS for any damage derived from, or in any other way related to this Agreement, whether contractual, extra-contractual or otherwise, will be limited to the amount of the fees that have been paid to VÍNTEGRIS for the Services regulated in the contract that gives rise to the liability during the twelve (12) month period immediately preceding the event that gave rise to said liability, less any refunds or credits that may have been received from VÍNTEGRIS under the contract, provided that it is not attributable to gross negligence or fraud of VÍNTEGRIS.

THIRTEENTH. Client Obligations

The Client must:

1. Ensure the maintenance of the installation for correct access to services and, if applicable, adapt it to the technological evolution of the contracted services.

2. Comply with VÍNTEGRIS instructions and those indicated in the documentation provided, if applicable.

3. Pay the economic consideration agreed upon in the Economic Proposal.

4. Facilitate the correct performance of activities by VÍNTEGRIS.

5. Do not provide user accounts and access to third parties. The Client will be responsible for the diligent and proper use of access to the contracted Service and/or Software.

6. It will ensure that its and its End Users' use of the Services, including all use of and access to Customer Data, complies with the provisions of these General Conditions, which shall act a diligent manner in the use of the services and will not be used to carry out any activity contrary to the laws, morals or public order or to use the services for fraudulent, illicit, prohibited purposes or that may cause injury to the interests of third parties, and VÍNTEGRIS declines any responsibility that may arise from these actions.

7. The data entered on the platform is legal and duly authorized to be stored and processed.

8. Inform VÍNTEGRIS of any fact or situation that may have occurred that could put the security of access by authorized users at risk.

9. It is prohibited to force failures or search for security breaches in the platform without express authorization from VÍNTEGRIS.

10. Do not subject the platform to workloads that are clearly aimed at destabilizing it, including denial of service (DDoS) attacks or similar situations. If this type of situation is detected, the level of service indicated above will not apply, and it will be considered an emergency situation.

11. Observe the restrictions established in the clauses relating to the license and Intellectual Property.

12. The Client will be responsible to VÍNTEGRIS and any third party in good faith for any damages resulting from the infringement, on their part, of the obligations established in these General or Particular Conditions.

FOURTEENTH: Intellectual property

Without prejudice to the provisions of clause NINTH, any computer program (Software) supplied, as well as all its documentation and/or information related to it, is the exclusive property of VÍNTEGRIS or, where applicable, of the VÍNTEGRIS Software Suppliers.

All intellectual property rights and copyright over the Program, the documentation, as well as any other work, program and/or product delivered by VÍNTEGRIS to the Client in compliance with the applicable agreements according to Clause Sixth, belong to VÍNTEGRIS or its Software Suppliers.

The Client will refrain from deleting, modifying or altering in any other way the mentions of reservation of rights in favor of the licensor, as well as, among others, the name, logo, or brand that identifies the latter entity in all documentation provided on any medium in the context of this Agreement or the applicable agreements according to Clause Sixth.

FIFTEENTH: Client Brands

By accepting these General Conditions, the Client authorizes VÍNTEGRIS to use its brand(s) and logo(s) (hereinafter, the "Brands") for the sole purpose of using it in commercial presentations to refer to the fact that it is a VÍNTEGRIS Client.

To this end, the Client authorizes VÍNTEGRIS to insert and communicate its Brands in all advertising and support media and materials as provided.

The Client authorizes the arrangement and configuration of its Marks so that they appear in the form and are placed appropriately for its image without altering colors, shapes, symbols, or graphics.

Thus, VÍNTEGRIS undertakes to (i) not alter, deface or mutilate the Brand(s) in any way; (ii) not use the Brand(s) in a way that damages the prestige or image of the Client; (iii) respect those reasonable instructions transmitted by the Client concerning the use of the Brand(s) for its protection and maintenance of its distinctive strength, renown, and homogeneity.

The use that VÍNTEGRIS makes of the Brand/s during the execution of the commercial agreement between both parties does not mean in any case that VÍNTEGRIS acquires any right over it/s.

The Client will always have the option to prohibit VÍNTEGRIS from using its brands as indicated in this clause. If you choose this option, you must notify VÍNTEGRIS of the non-use of its brands, as stipulated herein, in writing in physical or electronic format.

Upon termination of the commercial relationship between the Client and VÍNTEGRIS, the Client will immediately cease using the Brand(s).

SIXTEENTH: Protection of Personal Data

VÍNTEGRIS, as Data Controller, in compliance with current data protection regulations, informs you of the collection and processing of personal data that may be processed as a result of contracting the services included in these General Conditions:

Data of contact persons and data related to the management of contracted services: The identification and contact data that may be provided in the pre-contractual and contractual phase of this relationship will be processed for the purpose of managing the contracted service: providing the required information, incident management, administrative management, billing, sending information related to the services provided by VÍNTEGRIS. The basis for legitimation of these treatments is the pre-contractual / contractual relationship existing between both parties and the legitimate interest of VÍNTEGRIS to maintain relationships of any kind with the legal entity in which the affected party provides their services.

Data may be communicated to public bodies in compliance with legal obligations.

The data retention period will be established in the applicable regulations in force and, where appropriate, the data will be kept for the time necessary to prove the correct execution of the contract. Basic contact details may also be kept indefinitely for future commercial actions based on the interest of VÍNTEGRIS.

The interested party will inform VÍNTEGRIS of any changes that occur in the data provided, so that they can be kept up to date.

Data related to the issuance of certificates: If the services contracted with VÍNTEGRIS include the issuance of certificates from VÍNTEGRIS as a trusted service provider qualified, the personal data provided will be processed for the purpose of issuing and, where appropriate, revoking the certificate. The personal data processed correspond to the identification data of the certificate holders and the documents provided by them that prove their identity, as well as the attributes that may be included in the certificate.. In those cases in which the certificate requires, the data related to the position held in the company and/or the representation powers/condition, will be processed. In addition, contact information (email and mobile phone number) provided by the signatory will be processed, which is necessary for the certificate issuance process.

The data may be communicated to competent bodies and auditors in compliance with current regulations.

The basis for legitimation of this processing is the contractual relationship between both parties and compliance with current regulations applicable to the provision of trust services.

The data retention period will be 15 years from the date on which the certificate be extinguished, in accordance with the provisions of the applicable regulations.

Furthermore, based on Víntegris' legitimate interest and compliance with the requirements established in the regulations applicable to trusted service providers, the data collected for the issuance of the certificate may be processed for the purposes of conducting internal audits to verify the proper functioning of our processes and monitor the correctness of the actions taken. The data may be processed for these purposes the time required to meet audit requirements.

Furthermore, personal data necessary for internal management of invoicing issued certificates may be processed. The legal basis for this processing is the legitimate interest of the data controller in issuing invoices for the contracted certificates. The data retention period will be that established in the applicable regulations for accounting and tax purposes and for addressing claims arising from issued invoices. Data may also be processed for statistical purposes based on the legitimate interest of the data controller.

Data related to nebulaID (video identification): When issuing certificates, the identity validation process is carried out using nebula ID, the personal data collected in this process will be processed for the purpose of identifying and validating the applicant's identity. The personal data processed are: identifying data, images of identity documents, results of the OCR processing of the identity documents provided, video images recorded as proof of identity, including voice recordings, audit trails of the verification process, and data related to the applicant's circumstances and related to the certificate (nationality, position or representation in the company, etc.).

Although a facial recognition process is performed using biometric techniques, no biometric data are stored.

The video identification process and the personal data collected are those established in current regulations. This is the basis for legitimizing the processing, along with the data subject's consent, which is obtained before beginning the process. Data subjects are informed of the possibility of validating their identity through other means, such as in-person identity verification.

This data may be communicated to competent bodies and auditors in compliance with applicable regulations.

The data retention period is fifteen years from the expiration date of the issued certificate and five years when the validation process has failed and a fraud attempt is considered possible, counting from the date of the validation process, in accordance with current regulations.

Furthermore, based on Víntegris' legitimate interest and compliance with the requirements established in the regulations applicable to trusted service providers, the data collected for the issuance of the certificate may be processed for the purposes of conducting internal audits to verify the proper functioning of our processes and monitor the correctness of the actions taken. The data may be processed for these purposes the time required to meet the audit requirements.

Likewise, personal data may be processed as necessary for internal management of invoicing for issued certificates. The legal basis for this processing is the legitimate interest of the data controller in issuing invoices for the contracted certificates. The data retention period will be that established in the applicable regulations for accounting and tax purposes and for addressing claims arising from issued invoices. Data may also be processed for statistical purposes based on the legitimate interest of the data controller.

When any of the data processing operations indicated in this clause involve providing third-party data, the client must inform the data subject in advance of the terms set forth in this clause.

At any time, the interested party may request to exercise their rights recognized in the regulations on personal data protection,

by written and signed request, accompanied by a copy of their DNI or equivalent document that proves their identity, likewise, when acting through representation, it will be necessary to prove the existence of this representation. Applications should be addressed to VÍNTEGRIS:

:

a. By email:

incidentesRGPD@vintegris.com

b. By postal mail to the address of the Data Controller :

Pallars Street, 99
Floor 3
Office 33
08018 Barcelona

VÍNTEGRIS also reminds the interested party that they have the right to file a claim with the relevant supervisory authority (Spanish Data Protection Agency).

SEVENTEENTH: Data Retention and Deletion

At all times during the term of its subscription, the Client will be able to access, extract and delete the Client Data stored in the nebulaSUITE Service.

The Customer will have access to application audit logs for a period of 12 months. VÍNTEGRIS will continue to guard these records for a more extended period in those cases in which current legislation so determines. However, they will no longer be accessible by the Client through the platform.

VÍNTEGRIS will retain Customer Data that remains stored in the nebulaSUITE Services in an account with limited functionality for sixty (60) days following the expiration or termination of Customer's subscription so that the Customer can extract the data. After the expiration of the sixty (60) day retention period, VÍNTEGRIS will deactivate the Customer's account and delete the Customer Data and Personal Data within a period of an additional ninety (90) days, unless applicable law requires VÍNTEGRIS to retain These data.

In cases where, for some reason, the Client does not have any access to their account, VÍNTEGRIS will make available alternative mechanisms so that the Client's Data can be extracted.

VÍNTEGRIS will not incur any liability for deleting Customer Data or Personal Data, as described in this section.

EIGHTEENTH: Security Measures

VÍNTEGRIS guarantees in the provision of its services compliance with the security measures established in the eIDAS, NIS 2, ENS (High) regulations and in the ISO 27001, ISO 27017, ISO 27018 and ISO 27701 standards as accredited by our certifications in these regulations and security standards.

While VINTEGRIS is responsible for implementing security measures, certain security measures depend on the Client's management of them. To guarantee information security, the Client agrees to:

- User Management: VINTEGRIS will provide a user manager to the person designated by the Client as responsible. The Client's user manager will manage the creation, deletion, and modification of users within their tenant, with the Client being solely responsible for this management. The Client agrees to properly manage user access, specifically by deactivating (disabling) users who, due to a change in their role, no longer require access to the tenant or who leave the organization.

- Access Rights: The Client, through their manager user account, will grant access permissions to their users by assigning the different roles available in Nebula, as necessary for them to perform their functions.

The Client agrees to conduct a periodic review of the users with access to the tenant and their access rights.

- User Responsibility: The Client will guarantee the correct use of the created user accounts. User accounts will be assigned a specific name and sharing will not be permitted, thus ensuring traceability of the actions performed by each user.

The user will be responsible for the actions carried out with their identifier, and therefore should not allow the use of their user by third parties.

- Passwords and two-factor authentication: The Client will configure secure passwords and activate the use of two-factor authentication.

VINTEGRIS will not be responsible for any security incident affecting the information contained in the Client's tenant when the cause of this incident originates from a breach of the obligations established in this clause

NINETEENTH: Modifications

VÍNTEGRIS reserves the right to modify at any time the terms and conditions of these General Conditions and/or the Annexes included related to the Service, being applicable in the subsequent renewal of each Client's subscription. If the Client does not accept these new General Conditions, they must communicate the non-renewal of the subscription.

In the event that a change to these General Conditions is required for regulatory and/or legal reasons and these changes affect the use of nebulaSUITE services or the legal rights of the Client to our Services, VÍNTEGRIS will send the Client a notification before from the effective date via an email message to the address associated with your account. These updated Terms will come into effect no less than 30 days from the time we send you notice.

If the Client does not accept the changes that VÍNTEGRIS has implemented, VÍNTEGRIS will enter into a process of negotiation and dialogue with the Client to try to resolve the dispute. If the Client finally declines these changes, their account will be cancelled. In cases where this measure is applicable, VÍNTEGRIS will offer the Client a prorated refund based on the amounts they have already paid for the Services and the date of cancellation of their account.

TWENTIETH: Integrity

The clauses of these General Conditions are independent of each other, which is why, if any clause is considered invalid or inapplicable, the rest of the clauses will continue to be applicable unless expressly agreed otherwise by the parties.

TWENTY-FIRST: Documentation

It is expressly stated that a copy has been delivered, in electronic format (by making it available on the website), of all the documentation referred to in these General Conditions, as well as a copy thereof together with the Financial Proposal.

TWENTY- SECOND: Notifications

All notifications between the parties will be made in writing and delivered personally or in any other way that certifies receipt by the notified party. VÍNTEGRIS establishes the following address for notification purposes: administracion@vintegris.com.

Any change of address of one of the parties must be notified to the other immediately and by a means that guarantees receipt of the message.

TWENTY- THIRD: Applicable legislation and jurisdiction

In all matters not provided for in these general conditions, the agreement will be regulated by Spanish civil and commercial legislation. The competent jurisdiction is indicated in Law 1/2000, of January 7th on Civil Procedure. In the event of a discrepancy between the parties in relation to the interpretation or compliance with these General Conditions, the parties will attempt a prior amicable resolution in accordance with the procedure established by VÍNTEGRIS in this regard.

If the parties do not reach an agreement in this regard, any of them may submit the conflict to civil jurisdiction, subject to the Courts of the registered office of VÍNTEGRIS, except when the applicable Legislation establishes different mandatory rules.

TWENTY- FOURTH: Cessation of operations

In the event that VÍNTEGRIS decides to cease its operations, all reasonable efforts will be made to notify the Client as much as possible in advance and make available mechanisms for the recovery of their personal data and audit records.

TWENTY- FIFTH: Force majeure

VÍNTEGRIS will not incur in default or delay in its obligations to the extent that its performance is delayed or prevented by causes beyond its control, including, without limitation, acts beyond its control, such as acts of the Client; governmental restrictions (including the denial or cancellation of any export, import or other license; acts of third parties not under the control of VÍNTEGRIS; acts of any governmental body; pandemics; war, hostility, insurrection, sabotage or armed conflict; embargo, fire, flood, strike or any other labor disturbance; interruption or delay in transportation; unavailability or interruption or delay in telecommunications or third-party services; virus or hacker attacks; third-party software errors (including, without limitation, e-commerce software, payment systems, chat, statistics, or free scripts); as well as the inability to obtain raw materials, supplies, or energy or equipment necessary for the provision of the Services.

VÍNTEGRIS will use reasonable efforts to mitigate the effects of an event.

If such an event persists for over 30 days, either party may cancel the Services pending provision by written notice.

This clause does not relieve the parties of their obligation to take reasonable steps to follow their normal disaster recovery procedures or their obligation to pay for the Services.

TWENTY-SEVENTH: Entirety of the General Conditions

El Cliente acepta que estas Condiciones Generales y la información incorporada a las mismas en virtud de una referencia por escrito, y la propuesta económica correspondiente, constituyen la totalidad del acuerdo respecto de los Servicios que el Cliente solicite y reemplazan a todos los contratos o declaraciones anteriores o contemporáneos, sean escritos o verbales, relacionados con dichos Servicios.

Queda expresamente convenido que los términos de estas Condiciones Generales prevalecerán sobre los términos incluidos en cualquier orden de compra, portal de contrataciones en Internet o cualquier documento similar que no sea de VÍNTEGRIS, y ninguno de los términos incluidos en tal orden de compra, portal o documento similar que no sea de VÍNTEGRIS será aplicable a los Servicios solicitados.

En el caso de que los usuarios y Clientes de VÍNTEGRIS requieran realizar los pedidos a través de sus propias plataformas, las posibles condiciones de uso para dar de alta a los servicios o como proveedores no formarán parte del contenido contractual que se circunscribirá a las presentes Condiciones Generales, las cuales prevalecerán frente a otros términos previstos en las plataformas de Clientes que pudieran ser exigidas solo para tramitación del pago y de la petición de servicio a VÍNTEGRIS, aunque su firma y tramitación por VÍNTEGRIS sea posterior a la celebración del presente Contrato.

En caso de contradicción entre los términos de una Propuesta Económica y las Condiciones Generales, prevalecerán los términos establecidos en la Propuesta Económica al considerarse éstos parte de las Condiciones Particulares pactados y comprometidos entre ambas partes.

Excepto por lo autorizado en Propuesta Económica, Protección de Datos y la Cláusula de sitios web de terceros con respecto a los Servicios, las presente Condiciones Generales y las órdenes efectuadas en virtud de las mismas no pueden modificarse, y los derechos y restricciones no estarán sujetos a modificaciones o renuncias, a menos que se suscriba un documento por escrito o se acepte en línea a través de VÍNTEGRIS por los representantes autorizados de las partes. Las presentes Condiciones Generales no crean vínculos con terceros beneficiarios.

ANNEX I

Specific Terms of nebulaSUITE Services

1. nebulaUSERS Terms

1.1. Recogida de datos personales. La creación de nuevos usuarios conlleva la recogida de la siguiente información de carácter personal: nombre, apellidos, identificador de usuario, correo electrónico y teléfono (opcional). Esta información se trata conforme a lo especificado en la cláusula décima sexta de las Condiciones Generales de nebulaSUITE.

1.2. Integración con repositorio de usuarios corporativo. La información de carácter personal importada a nebulaUSERS desde los repositorios corporativos se utiliza y almacena de la misma manera que la información recogida directamente. En ningún caso se recupera de los sistemas corporativos del Cliente información que pudiese poner en riesgo la seguridad del usuario, tal como la contraseña.

1.3. Distribución de software propietario. Todo el software Cliente y/o documentación publicada en el portal nebulaUSERS sigue el modelo de licenciamiento y uso detallado en la cláusula octava de las Condiciones Generales de nebulaSUITE.

2. nebulaACCESS Terms

N/A

3. nebulaID Terms

3.1. Issuance of qualified certificates. To configure and activate the functionality for issuing qualified certificates of the VÍNTEGRIS certification entity in any of its modalities, the formalization of a specific contract between VÍNTEGRIS and the Client is required.

3.2. Service modalities. nebulaID is a product that allows you to create verified digital identities based on identity validation processes that enjoy the same legal recognition as personification. Depending on the nature of these validation processes, the product can be consumed in the following ways.

- **In person.** The registry operator verifies the identity of the certificate holder in person.

- **Unattended remote video identification**. The certificate holder is identified using biometric recognition technology. The registry operator unattended reviews process evidence and validates that process requirements are met before verifying the applicant's identity.

The unattended remote Video Identification modality is offered following the requirements established by current legislation on digital identification, as established by Order ETD/465/2021 of May 6, which regulates remote identification methods by video for the issuance of qualified electronic certificates.

In this modality, both VÍNTEGRIS' own technology and that of other technology providers are used internally.

3.3. Definition of identification process states and consumption metrics.

The different states of the identification processes in the Unattended Remote Video Identification modality are detailed below.

- **Process started**. Request to start an identification process in which the requesting user and the set of personal data to be verified are specified.

- **Video identification**. Autonomous process through which the requesting user provides evidence that allows his or her personal data and identity to be reliably validated.

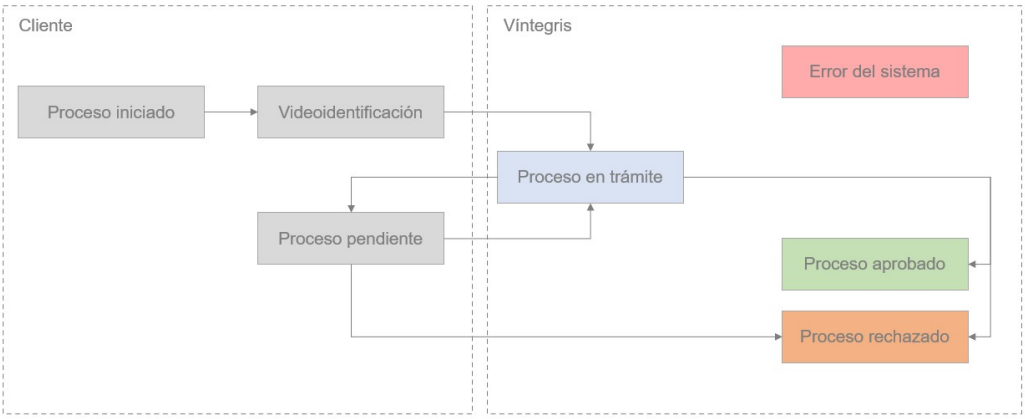
- **Process in process**. Review by a registry operator of the set of evidence resulting from the Video Identification process.

- **Pending process**. Request by the registry operator for additional information to the requesting user necessary to validate the process satisfactorily.

- **Approved process**. Approval by the registry operator of all the evidence provided allows verification of the identity of the requesting user, and in those cases where it is required, the issuance of a qualified electronic certificate is approved.

- **Process rejected.** Termination of the process due to not being able to comply with the minimum requirements that allow verifying the identity of the applicant due to i) the set of evidence does not allow the identity of the user to be guaranteed, ii) the user has not provided the additional information required correctly and/or in time.

- **System erro**r. Irregular behavior of the nebulaID product prevents any step of the identification process from being executed normally, resulting in its unexpected termination.



The different consumption metrics associated with the identification processes carried out in the video identification modality are described in this section below.

- **Contracted processes**. (Video identification number/package contracted). Set of processes approved within the contracted subscription period plus the set of irregular processes that exceed the minimum conversion percentage agreed upon (PCMA) between VÍNTEGRIS and the Client.
- **Approved processes**. Set of processes executed satisfactorily and that end with obtaining a verified identity and, where appropriate, the issuance of a qualified electronic certificate.
- **Irregular processes**. Set of processes that i) end in Rejected status or ii) end in approved status but require more than one iteration of the Video Identification process and/or request for additional information and documentation from the requesting user.

The processes contracted by the Client will, therefore, be accounted for as follows:

- Approved processes will subtract 1 from the total number of contracted processes.
- Irregular processes below the PCMA threshold will not be subtracted from the total number of contracted processes.
- Irregular processes above the PCMA threshold that end in Rejected status will subtract 1 from the total number of contracted processes.
- Irregular processes above the PCMA threshold that end in Approved status will subtract 2 from the total number of contracted processes.

If VÍNTEGRIS and the Client do not agree on a specific PCMA, this will be assumed to be 20%.

3.4. Service-Level Agreements (SLA) of the VÍNTEGRIS Registry Operator service.

The use of nebulaID in its Unassisted Remote Video Identification modality requires manual review of the biometric evidence by a registry operator, whose availability directly conditions the response time between the completion of the process by the requesting user and the at which time the user's identity is validated, and the issuance of the qualified electronic certificate or any other subsequent process can proceed.

This response time is regulated by a Service-Level Agreement or SLA between the Client and VÍNTEGRIS, which regulates the limit conditions under which each request is managed. This SLA is defined as follows.

- **Registration operation service availability** (Service Coverage). The time interval in which operators are available to respond to requests. Examples: 8x5, 12x7, 24x7

- **Maximum resolution interval or time** (Response Time). It is the maximum time that elapses before a request is resolved within the hours of availability of the operations service. This includes both approved and rejected processes, as defined in section 3.3. Examples: 1 hour, NBD (next business day), 1 week

  The resolution time for a request will begin to count only when the requesting user has completed the identification process and all the required documentation has been correctly attached.

- **Volume of requests processed** (Number of minimum video identifications). Minimum number of requests committed to review by registry operators within the maximum resolution interval.

The team of operators may process more requests according to availability, as long as it does not conflict with the SLA agreed with other Clients.

VÍNTEGRIS does not guarantee any SLA that has not been clearly previously reflected in an agreement between the two parties. This includes both the response times by the registry office, as well as the conversion percentages of the video identification process or availability of the video identification service.

4. nebulaCERT Terms

4.1. Use of qualified certificates. It is the Client's responsibility to use their qualified digital certificates in accordance with the provisions of the trust service provider issuing them. The conditions of use of the certificates are detailed in the “acceptance sheet” or contract that the certificate holder signs at the time of delivery, and said use must be in accordance with the

applicable Law, including any Laws that regulate the authentication of certificates, signature and the delegation of signature. VÍNTEGRIS will not be responsible for the consequences of non-compliance with the contract between the certificate holder and the issuing certification entity, or for any improper use of a certificate and its associated private key by its holder.

5. nebulaSIGN Terms

5.1. Signature formats. nebulaSIGN allows the generation of the most common signature formats, among which are the CAdES, PAdES and XAdES formats in their different modalities. Detailed information about the different recognized signature formats can be consulted on the electronic administration portal:

http://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html

6. nebulaSNE Terms

N/A

7. nebulaDISCOVER Terms

7.1. Collection of personal data. The following personal information is collected during the registration process: name, surname, company, and email. This information is treated in accordance with what is specified in clause sixteen of the General Conditions of nebulaSUITE.

ANNEX II

Service-Level Agreements (SLA)

This nebulaSUITE Services Service-Level Agreement ("SLA") is a policy that governs your use of nebulaSUITE and applies separately to each service. In the event of a conflict between the terms of this SLA and the General Conditions, the terms and conditions of this SLA apply, but only to the extent of such conflict. Terms used herein and not defined here will have the meanings set forth in the General Conditions.

Definitions

- **Error Rate:** (i) the total number of internal server or service availability errors returned by each service divided by (ii) the total number of requests during a five-minute period. The Error Rate for each nebulaSUITE account and for each service separately will be calculated as a percentage for each five-minute period in the billing cycle. The calculation of the number of internal server or service availability errors will not include errors that arise directly or indirectly as a result of any exclusion from the SLA of the services, as defined below.

- **Average Service Availability Percentage (PDSM):** This is calculated as the difference between 100% of the average error rates for each five minutes of the billing cycle, whatever it may be.

Support

VÍNTEGRIS provides the CLIENT with a technical support team of engineers with extensive experience in information systems security, digital certificates and electronic signatures with sufficient knowledge and training to offer a personalized and quality support service.

The support service is available through different modes of use by the CUSTOMER: Standard Support, Plus Support and 24×7 Plus Support.

- **STANDARD SUPPORT** – is included by default and at no additional cost with all nebulaSUITE service subscriptions.

  Standard Support is available during the active subscription period if you are up-to-date with your payment.

  - In 10×5 mode, from Monday to Friday (except national holidays), from 8:30 a.m. to 6:30 p.m.

- Includes access to the support portal (https://vintegris.zendesk.com/) and the nebulaSUITE resources and documentation portal
- The interaction with the support team always begins from the support portal and continues either through said portal, via email, or in remote collaborative sessions via teleconference.
- Incidents must always be opened by a nebulaSUITE technical user/administrator in the CLIENT's organization. Requests created by CUSTOMER end users are not supported.
- Support is provided for product incidents due to malfunctions of our intellectual property, development defects, unavailability of cloud components, etc.
- **Standard Support does not include**, in any case:
  - Support at the CUSTOMER location
  - Code design or development
  - Support for testing integrations, customizations and/or modifications
  - Management of change or improvement requests in nebulaSUITE
  - Support or any action regarding third-party software included in the Services
  - Support for applications developed and/or owned by the CLIENT
  - Support for incidents caused by important changes in the Software configuration by the CUSTOMER
  - Errors attributable to lack of diligence or responsibility of the CUSTOMER
  - Consulting or training services
  - Custom documentation
  - Responsibility for changes or replacement of Client's hardware/software that may be necessary to properly use VÍNTEGRIS intellectual property due to a workaround, fix or new version.

Process to follow to report an incident:

- When notifying a new incident, the client must provide VÍNTEGRIS with the following data through the Support Portal (https://vintegris.zendesk.com/):

  - CUSTOMER name and code. It is necessary to have a CUSTOMER code to open a ticket in the Support Portal
  - CLIENT contact information: Name, email and telephone number of the contact person
  - Data on the affected product
  - Product version or modules affected
  - System/architecture detail: OS version, etc.
  - Detailed description of the incident
  - Scope of the impact of the incident:
    - Affected environment (Productive, non-productive environment or isolated case)
    - Urgency or criticality

- The CUSTOMER user responsible for creating an incident will be available to respond to requests for information, tests, or direct collaboration that support engineers may need to diagnose the incident.
- If the CLIENT does not provide the data or test results required by the support engineers within 5 business days or does not respond to any other requirement, the incident will be closed, although the option will be given to reopen it if necessary.
- The response time, depending on the severity of the incident opened in Standard Support, is as follows:

Severity	Incident Type[1]	Max Time Response[2]	Contact Method
Severity 3	Isolated incidents with low-impact Product incidents that affect Test, Trial or Pre-Production environments.	2 business days	Support Portal with tracking via portal and email
Severity 2	Product incidents that do not affect a Productive environment or that do not have significant impact or urgency. Incidents of the product that prevent its use sporadically or individually by users.	1 business day	Support Portal with tracking via portal and email

[1] **Incident Type**: When the incidents created by the CUSTOMER do not fit the description corresponding to their severity according to this table, the support team may change the severity level according to it at its discretion.

[2] **Maximum Response Time**: It is the maximum time established during which the VÍNTEGRIS support staff will contact the CUSTOMER to collect data regarding the product incident and assign personnel for analysis and resolution.

Severity 1	Critical incidents affect the productive environment with significant impact or urgency. Product issue that prevents core product functions from being performed on all workstations or users (high impact)	4 working hours	Support Portal with tracking via portal and email

- **PLUS SUPPORT** - available only through specific contracting by the CUSTOMER

  It is possible to contract Support Plus if there is an active and paid nebulaSUITE subscription.

  SUPPORT PLUS is a service offered explicitly by VÍNTEGRIS to specific CUSTOMERS under the criteria of VÍNTEGRIS.

  The Support Plus service contracted must always be within the nebulaSUITE subscription period contracted.

  Support Plus includes all the features of Standard Support and adds the following features:

It has an exclusive portal for reporting incidents and Support Plus[3] requests.

- Expand the scope of service by offering[4]:
  - Resolution of doubts about the use or operation that Standard Support does not cover
  - Direct support to the CUSTOMER in specific service operation tasks in their corporate environments, even if they are not caused by incidents or malfunctions of nebulaSUITE or any of its components.
  - Direct support for updating and configuring on-premise service components, with the client responsible for the subsequent mass distribution of these components, if necessary, such as the mass distribution of the nebulaCERT agent in workplaces
  - Support for specific questions about the development of integrated applications using the nebulaSUITE REST API

[3] Plus Support requests will be handled under the same SLA as standard support. The resolution period for these requests will vary depending on their nature and will be managed through the ticket. The procedure to follow to register an incident covered by standard support is the same as indicated above for this support type.

[4] Consult the corresponding section for detailed information on tasks and services included and excluded in each of the listed categories.

- Helps users and operators in the application, approval, and issuance of VÍNTEGRIS certificates

To contract this service, it is necessary to contact Víntegris.

- **PLUS SUPPORT 24×7** - Available only through specific contracting by the CUSTOMER

  It is possible to contract SUPPORT PLUS 24x7 as long as there is an active and paid nebulaSUITE subscription.

  SUPPORT PLUS 24x7 is a service offered explicitly by VÍNTEGRIS to specific CUSTOMERS under the criteria of VÍNTEGRIS.

  The contracted SUPPORT PLUS 24x7 service must always be within the contracted nebulaSUITE subscription period.

  - To provide the SUPPORT PLUS 24x7 service, VÍNTEGRIS makes available to its clients a team of support engineers and DevOps engineers trained for urgent diagnosis and resolution, outside of working hours, of most incidents that arise that can cause the unavailability of a critical service.
  - SUPPORT PLUS 24x7 includes all the features of Standard Support and Support Plus and adds the following features:
  - 24×7 mode at any time of the day, including holidays only for Severity 1 incident
  - Direct telephone hotline for reporting Severity 1 incidents every day of the week at any time of the day (24×7)
  - [5]The CLIENT's previously designated interlocutors may have the support activated in 24×7 mode only when they are experiencing a problem of malfunction or unavailability of the nebulaSUITE service or any of its components due to technical issues originated by/in nebulaSUITE that cause the client's users so they cannot carry out their work or that it is carried out poorly and prevents the performance of the functions of these users globally in the client's organization.
  - Our 24×7 Support teams will request additional documentation of the critical incident from the customer through the support portal for documentary purposes and as a monitoring mechanism for the life cycle of this issue.
  - If the incident managed through 24×7 Support requires modification of the nebulaSUITE code or any of its components for its solution, the VÍNTEGRIS development team will carry this out within normal working hours.
  - Specific SLA for 24×7 Support requests:

[5] It is recommended to use the telephone hotline only outside normal working hours, since the usual channels already allow the management of critical incidents in this period

Severity	Incident Type	Max Time Response[6]	Contact Method
Severity 1	Critical incidents affect the productive environment with significant impact or urgency. Product issues that prevent core product functions from being performed on all workstations or users (high impact). .	2 hours	By telephone through the CUSTOMER's previously designated interlocutor

To contract this service, it is necessary to contact VÍNTEGRIS.

Detailed scope of Support Plus coverage

Through the Support Plus service, VÍNTEGRIS provides clients with a help and collaboration service that goes beyond the Standard Support included by default with each nebulaSUITE subscription or any of its components.

It is aimed at those clients who make intense, functional or frequent use of nebulaSUITE in organizations, mainly through:

- nebulaSUITE administrators
- nebulaCERT certificate owners
- Programmers using the REST-API
- VinCAsign Registration Authority Operators via nebulaID
- Users requesting vinCAsign certificates

This service is not intended to be a managed service that replaces the work that each of the previous groups performs in the CLIENT's organization, but rather an assistance tool to be able to resolve doubts or carry out actions for which, due to their specialized nature or, Simply, ignorance, they are not initially trained.

Therefore, unless otherwise determined by the support team, all service actions provided through Support Plus will require the active collaboration of at least the person requesting it and the tasks

[6] **Maximum Response Time**: It is the maximum time established during which the VÍNTEGRIS support staff will contact the CUSTOMER to collect data regarding the product incident and assign personnel for analysis and resolution.

necessary for its implementation. Execution will be done through direct interaction between support staff and this person.

Likewise, although the actions carried out with the applicants will, as far as possible, be educational in nature so that the applicant user can improve their training in using our technology, Support Plus is not a training service nor a tool to create specific documentation for CUSTOMER users.

The technical capabilities of nebulaSUITE will limit all service actions under Support Plus while providing the specific service. It will be indicated promptly if the request cannot be attended to because it exceeds them or is outside the functional scope of our solution.

On-premise components for which specific actions are required must use officially supported versions; If not, updating these will be coordinated with the CUSTOMER.

Details of tasks included in Support Plus

- Resolution of extended use or operation questions not covered by Standard Support.
  - Address any doubt or technical question about the operation and use of nebulaSUITE and its components.
  - As far as possible, always respond based on the documentary base of the nebulaSUITE product and user manuals to make this material known to users and familiarise them with its use.
  - If the request exceeds what is stated in the nebulaSUITE manuals, it may need to be transferred to another team before the requester can respond.
- Directly support the CUSTOMER in specific service operation tasks in their corporate environments, even if they are not caused by incidents or malfunctions of nebulaSUITE or any of its components.

  Among others, the following types of actions are included:
  - Creation and configuration of users and groups in nebulaUSERS
  - General and security configuration of the corporate nebulaSUITE environment
  - Help with importing certificates in nebulaCERT
  - Help with creating certificate policies, ACLs and Navigation Cycles in nebulaCERT
  - Help with nebulaSIGN signing flows and step configuration
  - Configuring SAML Federation with Corporate IDP
- Provide direct support for the update and configuration of on-premise components of the service:
  - nebulaCERT agent on Windows workstations
  - SSO components for integrated authentication with Active Directory
  - Active Directory User and Group Synchronizer
  - Authentication Bridge for authentication integrated with Active Directory
  - Local KeyCave for key storage in corporate infrastructure (with and without HSM)
- Provide support for the development of integrated applications using the nebulaSUITE REST-API
  - Specific help requests for using nebulaSUITE functionalities through its REST API
  - Providing examples using Postman

- Helps users and operators in the application, approval, and issuance of VÍNTEGRIS certificates
  - Helps CLIENT operators in creating requests for new certificates
  - Resolution of procedural doubts and documentation required for the approval of applications, depending on the types of certificates
  - Helps end users in the processes of video identification, issuance, and download of certificates

To guarantee the availability of the Support Plus service for all customers, there are logical limits to using this service. These limitations appear in the CLIENT's particular contract conditions.

Service Evolution

VÍNTEGRIS provides software maintenance and update services, which consist of a new version of the software that eliminates existing errors in the current version or improves the software.

VÍNTEGRIS reserves the right to suspend, totally or partially, the contracted service if it notices, detects and/or verifies in its maintenance work any alteration that slows down or leads to impairment in the provision of the service or the rights of Clients or third parties; as well if a risk or vulnerability to the security of the Service is detected.

VÍNTEGRIS reserves the right to proceed to unilaterally update or improve its solutions without affecting any additional cost to the current subscription, without prejudice to the negotiation of the renewal of the subscription.

The Client undertakes to provide VÍNTEGRIS, without being requested, all the information necessary for the correct evaluation and execution of the corresponding service request to verify and know the possible causes related to the conditions of its operating system and other elements that may affect navigation.

Furthermore, the Client is obliged to install the updates made available by VÍNTEGRIS and to use only the most current version of the software or the one immediately preceding it.

VÍNTEGRIS will not be responsible for actions derived from or damages caused by the operation of the Platform due to it not meeting the Client's expectations or when they may be due to problems caused by the Client's systems and assets.

Service Availability

Unless otherwise specified in the particular clauses of each service, VÍNTEGRIS Cloud services are available 24 hours a day, 7 days a week.

VÍNTEGRIS will use commercially reasonable efforts to ensure the availability of the services with an Average Service Availability Percentage or PDSM of at least 99.5%, excluding justified Downtime. VÍNTEGRIS will monitor the availability of the Service in an automated manner 24 hours a day, 7 days a week.

In the event of a planned service unavailability due to a platform update, VÍNTEGRIS will notify its Clients in advance, indicating the reason for the service outage, day, time slot and affected services. Therefore, it is the Customer's responsibility to keep their contact information updated for notifications throughout the duration of the Services.

Update Frequency

Product updates do not have a specific frequency. If the availability of the Service is affected, we will notify you in accordance with the previous section.

SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension, or termination of any of the services or any other performance problem thereof: (i) resulting from a suspension; (ii) caused by factors beyond the reasonable control of VÍNTEGRIS, including any force majeure event or Internet access or related problems beyond its point of demarcation; (iii) resulting from any action or omission on the part of the Client or a third party; (iv) resulting from Client personnel, software or any other technology and/or equipment, software or technology of a third party (other than third-party equipment that is under the direct control of VÍNTEGRIS; (v) resulting from a suspension and termination of the Customer's right to use the services in accordance with the service contract; (vi) that affects test, development, pre-production environments or environments for commercial purposes.

ANNEX III

(Data Processing Agreement VINTEGRIS 2022-ES.Rev.1.3_rev)

Data Processing Agreement ("DTA") for Víntegris nebulaSUITE services

This Data Processing Agreement ("DTA") is an agreement between the ("Client") and Víntegris, S.L. ("VÍNTEGRIS"). It establishes the obligations of both parties regarding the processing and security of personal data for which the Client is responsible concerning the use of the nebulaSUITE Services.

This ATD complements the General Conditions of the nebulaSUITE Service available at https://www.vintegris.com/es/nebulasuite-service-terms/ or another agreement between the Client and VÍNTEGRIS that governs the use by the Client of nebulaSUITE Services provided by VÍNTEGRIS when Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and the free circulation of this data ("GDPR").

This agreement does not cover any processing of personal data that VINTEGRIS VÍNTEGRIS may carry out as Data Controller when contracting services related to its status as a trusted service provider and whose processing of personal data is established in the sixteenth clause.

DEFINITIONS

For the purpose of this ATD:

- **"Applicable data protection law"** means the applicable laws and regulations where data processing takes place, which apply to the terms of this ATD and which may vary over time. Understand both Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data ("GDPR") such as applicable local laws where the treatment takes place.

- **"Controller"** or "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- **"Processor"** or "Processor" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller;

- **"Data subject"** means a person who is the subject of personal data.

- **"ATD",** "this ATD", "this ATD agreement" is this Data Processing Agreement;

- **"Personal data"** means any information about an identified or identifiable natural person ("the data subject"). An identifiable natural person is any person whose identity can be determined, directly or indirectly, in particular using an identifier, such as a name, an identification number, location data, an online identifier or one or more elements specific to identity. Physical, physiological, genetic, mental, economic, cultural or social of said person;

- **"Supervisory authority"** means an independent public authority established by a Member State that is responsible for supervising the processing of personal data to protect the fundamental rights and freedoms of natural persons regarding the processing of their data.

- **"Customer Data"** means all personal data (including personal data collected in the digital certificates) that authorized persons of the Customer incorporate into the databases and hosting systems of each service, as well as those that can be generated and preserved through the use of nebulaSUITE services. The Client is responsible for processing this personal data.

- **"Services"** and "nebulaSUITE Services" are Software as a Service (SaaS) services. These are the services provided over the internet by VÍNTEGRIS to the Client in relation to the use of the contracted service through the nebulaSUITE platform and within the cloud computing infrastructure.

- **"Subprocessors"** are any natural or legal person, public authority, agency or other body contracted by a data processor to provide part or all services subject to a processing order. The data controller authorizes any subcontracting of services derived from a processing order. In the processing assignment regulated by this ATD, subprocessors are the processors that Microsoft uses to process Customer Data, Professional Services Data and Personal Data, as described in Article 28 of the GDPR.

TERMS

SECTION I

Clause 1. Purpose and scope of application

(a) The purpose of the clauses of this ATD (in the future referred to as the "Clause Specification") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 of April 2016, relating to the protection of natural persons with regard to the processing of personal data and the free circulation of this data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have consented to be bound by this document to ensure compliance with Article 28, paragraphs 3 and 4, of Regulation (EU) 2016/679.

(c) This document of clauses applies to processing personal data specified in Annex II.

(d) This document of clauses is understood without prejudice to the obligations to which the person responsible is subject under Regulation (EU) 2016/679.

(e) The clauses of this ATD are aligned with the Commission Implementing Decision (EU) 2021/915 of June 4, 2021, on standard contractual clauses between controllers and processors.

(f) This ATD, including its definitions, recitals and annexes, is a stand-alone document that does not incorporate commercial terms that the parties must have established in separate commercial agreements.

Clause 2. The invariability of the terms and conditions

(a) The parties agree not to modify the specifications except to add or update information in the annexes.

(b) This does not prevent the parties from adding additional clauses or guarantees as long as they do not directly or indirectly contradict the terms and conditions or harm the fundamental rights or freedoms of the interested parties.

Clause 3. Interpretation

(a) When terms defined in Regulation (EU) 2016/679 are used in this clause, they are understood to have the same meaning as in the corresponding Regulation.

(b) This document of clauses must be read and interpreted under the provisions of Regulation (EU) 2016/679.

(c) Interpretations of this document of clauses may not be made that conflict with the rights and obligations established in Regulation (EU) 2016/679 and/or harm the fundamental rights or freedoms of the interested parties.

Clause 4. Hierarchy

In the event of a contradiction between this document of clauses and the provisions of related agreements between the parties that were in force at the time when this document of clauses was agreed or began to be applied, this document of clauses shall prevail.

SECTION II. OBLIGATIONS OF THE PARTIES

Clause 5. Description of the treatment or treatments

Annex II specifies the details of the processing operations and, in particular, the categories of personal data and the purposes for which personal data are processed on behalf of the controller.

Clause 6. Obligations of the parties

6.1. Instructions

(a) The controller shall instruct the processor to process the personal data in a manner reasonably necessary for the processor to carry out the processing in accordance with this ATD and under Regulation (EU) 2016/679.

(b) The processor will process personal data only following documented instructions from the controller in accordance with the terms of service set out in the nebulaSUITE General Conditions of Service unless obliged to do so under Union or Member State law applicable to the in charge. In such case, the processor will inform the person responsible for this legal requirement prior to processing unless such Law prohibits it for important reasons of public interest. The controller may also give further instructions at any time during the processing of personal data. These instructions must always be documented.

(c) The data controller will refrain from providing instructions that do not comply with applicable laws, including Regulation (EU) 2016/679, and if such instructions are given, the data processor has the right to desist from carrying them out.

(d) The processor shall immediately inform the controller if the instructions given by the controller infringe, in the opinion of the processor, Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or the applicable provisions of Union or State law members regarding data protection.

(e) The processor will not disclose any personal data to a third party under any circumstances other than at the specific written request of the controller unless such disclosure is necessary to fulfil the obligations of the Service Agreement or is required under Union Law or of the Member States that applies to the processor.

6.2. Limitation of purpose

The processor will process personal data only for the specific processing purposes indicated in Annex II, except when following additional instructions from the controller.

6.3. Duration of personal data processing

The processing by the processor will only be carried out during the period specified in Annex II.

6.4. Safety of treatment

(a) The information system that supports the services provided by Vintegris is certified under the National Security Scheme (HIGH category) and the ISO 27001, 27017, 27018 and 27701 standards. Vintegris will make the corresponding certificates of these standards available to the Client when required.

(b) The technical and organizational security measures applied to the processing of data subject to the provision of the service are those established in the standards set out in section (a).

(c) The data controller considers the security measures implemented by Vintegris to be adequate.

(d) The processor will only grant access to the personal data processed to members of its staff to the extent that it is strictly necessary for the execution, management, and monitoring of the contract.

(e) The processor will ensure that the persons authorized to process the personal data received have committed respect to confidentiality or are subject to a confidentiality obligation of a statutory nature. The processor must keep all documented records of compliance with the obligation of confidentiality at the disposal of the data controller.

(f) The processor must ensure that all persons authorized to process personal data receive the necessary training in personal data protection.

6.5. Sensitive data

If the data processing carried out by Vintegris, as the data processor, affects sensitive data, the data controller will be solely responsible for complying with the requirements established in current data protection regulations in order to process this data.

6.6. Documentation and compliance

(a) The parties must be able to demonstrate compliance with the clauses of this ATD.

(b) The processor will promptly and appropriately resolve the controller's queries related to the processing in accordance with this document.

(c) The processor will designate in Annex I, a point of contact within its authorized organization to respond to queries related to the processing of Personal Data and will cooperate with the controller, the Data Subject and the Supervisory Authority regarding all queries within a reasonable time.

(d) The person in charge will make all the information necessary to demonstrate compliance with the obligations contemplated in this document of clauses that derive directly from Regulation (EU) 2016/679.

(e) At the request of the controller, the processor will allow and contribute to audits of the processing activities covered by this document at reasonable intervals or if there are indications of non-compliance. When deciding whether to perform an audit, the controller may take into account any relevant certifications held by the controller that prove compliance with their obligations verified by an independent third party.

These audits will be requested with reasonable notice and conducted during regular business hours of the processor. The request may be subject to any necessary consent or approval from a supervisory authority within the country of the controller.

The cost of the audit, when performed by a third party designated by the Client, will be borne entirely by the Client. If the audit is performed by third parties contracted by the Client, there may be no conflict of interest with Vintegris.

(f) Audits must be limited exclusively to the Client's services and information, and access to third-party information is prohibited. The Processor's procedures and regulations are for internal use only and are confidential; therefore, copies of these documents may not be made during audits, except for those sections agreed upon with Vintegris.

The parties will make available to the competent control authorities, at their request, the information referred to in this clause and, in particular, the results of the audits.

(g) The processor will notify the data controller of any request for information from the Supervisory Authority.

(h) The processor will notify the responsible of any complaint, notification, or communication received that is directly or indirectly related to the processing of personal data or other related activities or that is directly or indirectly related to the compliance of the processor and/or the person responsible with the relevant applicable law, including applicable data protection law.

6.7. Use of sub-processors

(a) The processor has the authorization of the controller to hire subprocessors who appear on an agreed list documented in Annex IV. The processor will inform the controller specifically and in writing of the additions or substitutions of subprocessors provided for in said list at least one month in advance so that the controller has sufficient time to object to such changes before the subprocessor is hired or sub-processors in question. The person in charge of the treatment will provide the controller with the necessary information so that he can exercise his right to object.

(b) When the processor engages a subprocessor to carry out specific processing activities (on behalf of the controller), it will do so using a contract that imposes on the subprocessor, in essence, the same data protection obligations as those imposed on the subprocessor commissioned under this document of clauses. The processor will ensure that the subprocessor complies with the obligations to which he is subject under this contract document and Regulation (EU) 2016/679.

(c) At his request, the processor will provide the controller with a copy of the contract with the subprocessor and any subsequent modifications. To the extent necessary to protect trade secrets or other confidential information, such as personal data, the processor may redact the contract text before sharing the copy.

(d) Where it is not possible to sign a specific contract with the sub-processor, the terms and conditions for contracting its services established by the sub-processor must be adjusted and comply with the necessary guarantees of compliance with Regulation (EU) 2016/679.

(e) The processor will remain fully responsible to the controller for compliance with the obligations imposed on the subprocessor by its contract with the processor. The processor will notify the person responsible for the treatment of non-compliance by the sub-processor with the obligations attributed to him by said contract.

6.8. International transfers

(a) Data transfers to a third country or an international organization by the processor may only be carried out following documented instructions from the controller or according to an express requirement of Union or Member State law to which the processor is subject; they will be carried out under Chapter V of Regulation (EU) 2016/67.

(b) The controller agrees that where the processor uses a sub-processor under clause 6.7 to carry out specific processing activities (on behalf of the controller) and such activities involve a transfer of personal data within the meaning of Chapter V of the Regulation (EU) 2016/679, the processor and the subprocessor can ensure compliance with Chapter V of Regulation (EU) 2016/679 using standard contractual clauses adopted by the Commission, under Article 46(2) of Regulation (EU) 2016/679) 2016/679, provided that the conditions for the use of said standard contractual clauses are met.

Clause 7. Obligations of the data controller

The data controller guarantees and undertakes that:

(a) Personal data has been collected, processed and transferred by applicable data protection laws.

(b) You must evaluate the impact on the protection of personal data of the processing operations that the processor will carry out when the type of processing may give rise to a high risk for the rights and freedoms of the interested parties.

(c) It will have appropriate technical and organizational measures to protect the confidentiality of personal data, as well as against accidental or unlawful destruction, accidental loss, alteration, disclosure, or unauthorized access, and that provide a level of security appropriate to the risk posed, representing the processing and nature of the data to be protected.

(d) Respond to requests from data subjects and supervisory authorities regarding the processing of personal data as stipulated in Clause 8 (b).

(e) Make prior inquiries to the supervisory authority where a data protection impact assessment indicates that the processing would give rise to a high risk in the absence of measures taken by the controller to mitigate the risk.

Clause 8. Collaboration with the person responsible for the treatment

(a) The manager will promptly notify the person in charge of the requests received from the interested party. He will not respond to such a request himself unless the person responsible has authorized him to do so.

(b) The processor will collaborates with the controller in the fulfilment of his obligations related to the management of the requests for the exercise of rights of the interested parties, forwarding any requests received as soon as possible and, where appropriate, providing the necessary information or, when requested by the responsible party, taking the necessary actions to comply with the exercise of these rights.

(c) In addition to the processor's obligation to assist the controller under clause 8(b), the processor will also will collaborate with the controller in ensuring compliance with the following obligations, considering the nature of the processing and the information available to the processor.

1. the obligation to carry out an assessment of the impact of processing operations on the protection of personal data ("impact assessment") when a type of processing is likely to pose a high risk to the rights and freedoms of natural persons;
2. the obligation to consult the competent supervisory authorities before processing where a data protection impact assessment shows that the processing would entail a high risk if the controller does not take measures to mitigate it;
3. the obligation to ensure that personal data is accurate and up-to-date, informing the controller without delay if the processor discovers that the personal data he is processing is inaccurate or has become obsolete;
4.

(d) The parties will establish in Annex III appropriate technical and organisational measures that oblige the processor to assist the controller in applying this clause, as well as the purpose and scope of the assistance required.

Clause 9. Notification of personal data security breaches

In the event of a violation of the security of personal data, the processor will notify the controller within a maximum of 36 hours of any possible security incident affecting personal data owned by the controller and will collaborate with the controller in managing the incident until its resolution, as well as in preparing the reports necessary for the supervisory authority.

SECTION III. FINAL PROVISIONS

Clause 10. Non-compliance with the clauses and termination of the contract

(a) Without prejudice to the provisions of Regulation (EU) 2016/679, in the event that the person in charge of the treatment fails to comply with the obligations attributed to him in this document of clauses, the person responsible may order the person in charge to suspend the processing of personal data until this once again complies with this document of clauses, or terminates the contract. The person in charge will promptly inform the person responsible if he cannot abide by this document of clauses for any reason.

(b) The person responsible will be empowered to terminate the contract regarding the processing of personal data under this document of clauses when;

1) the controller has suspended the processing of personal data by the processor under letter a) and compliance with this document of clauses is not repeated within a reasonable period and, in any case, within a period of one month counting from suspension;

2) the person in charge substantially or persistently fails to comply with this document of clauses or the obligations attributed to him by Regulation (EU) 2016/679;

the processor fails to comply with a binding resolution of a competent court or the competent supervisory authorities concerning the obligations attributed to them by this document, Regulation (EU) 2016/679.

(c) The processor will be entitled to terminate the contract concerning the processing of personal data under this document of clauses when after having informed the controller that his instructions violate the legal requirements required by clause 7.1, letter b), The person in charge insists that these instructions be followed.

(d) After termination of the contract ,the deletion of the data will be carried out in accordance with the provisions of the General Terms and Conditions of contracting nebulaSuite services.

(e) Other reasons and conditions for the termination will be subject to the nebulaSUITE General Conditions of Service.

Clause 11. Liability and compensation

(a) The person in charge of the treatment will not be responsible for any claim presented by an interested party that is a consequence of any action of the person in charge to the extent that said action is the direct result of the instructions of the person in charge and the incorrect implementation of its technical and organizational measures.

(b) In the event that a data subject files a claim against the processor arising from any action or omission of the processor to the extent that such action or omission is the direct result of the controller's instructions or the incorrect application by the controller of its and organizational measures, under Clause 7 (c) of this ATD, the controller will indemnify and keep indemnified and defend at its expense the processor respecting all costs, claims, damages, or expenses incurred by the processor for which The controller may be liable for any breach by the controller or its managers, employees, agents, or contractors of their obligations under the provisions of this DPA.

Clause 12. Legislation applicable to this ATD

This ATD shall be governed by and construed in all respects under the laws and regulations of the EU country where the data processing occurs. The parties to this agreement submit to the exclusive jurisdiction of the place where the data processing takes place for all purposes of this ATD.

Clause 13. Resolution of disputes with interested parties or supervisory authorities

(c) In the event of a dispute or claim brought by a data subject or a supervisory authority regarding the processing of personal data against one or both parties, the parties shall inform each other of such disputes or claims and cooperate to resolve them amicably and in the most opportune way.

(d) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or a supervisory authority. If they participate in the proceedings, they may choose to do so remotely (for example, by telephone or other electronic means). The parties also agree to consider participation in any other arbitration, mediation, or other dispute resolution procedure enabled for data protection disputes.

(e) Each party undertakes to abide by the decision of the supervisory authority, which is final and against which it will no longer be possible to appeal.

ANNEX I. List of parts

As Data Controller:

Name: The Client who contracts the services of nebulaSUITE under the agreed General Conditions of Service.

Address: As specified in the agreement or contract for the provision of nebulaSUITE services signed between both parties.

Reference department/employee: As specified in the nebulaSUITE service provision agreement or contract signed between both parties

Name, position and contact information of the contact person: As specified in the agreement or contract between both parties

Date of accession: Date of entry into force of the contract or agreement for the provision of nebulaSUITE services signed by both parties

As Data Processor:

Name: VÍNTEGRIS, S.L.

Address: Calle Pallars, 99, Floor 3, Office 33, 08018 Barcelona, Spain

Reference department/employee: As specified in the nebulaSUITE service provision agreement or contract signed between both parties

Contact information for the contact person: incidentesRGPD@vintegris.com

Date of accession: Date of entry into force of the contract or agreement for the provision of nebulaSUITE services signed by both parties

ANNEX II. Treatment description

Personal data will be processed for the purpose of providing the nebulaSuite services described in Annex I of the General Terms and Conditions contracted by the Client.

Services contracted by the Client that are related to services provided by Vintegris in its capacity as a Qualified Trust Service Provider are excluded.

With regard to the provision of trust services, a data processing agreement will only be considered to exist when the Client is a Qualified Trust Service Provider (QTSP) and contracts Vintegris's services as its delegated Data Processor.

Categories of data subjects whose personal data are processed

Depending on the services contracted:

- Staff, collaborators, and others authorized by the Client who are users of the nebulaSUITE platform
- Holders of certificates that the Client manages through nebulaSUITE services
- Qualified certificate issuance applicants through remote video identification using the nebulaID platform.

Categories of personal data processed

Depending on the services contracted:

- Information of users of the nebulaSUITE platform necessary to access and use the services
  - Identity of the users, for example, their first and last names
  - Professional contact information such as email address and telephone number
  - Authentication data for access
  - Records of user activity in the use of the Services, which may include information on the IP address from which the nebulaSUITE platform is accessed

- Data of the holders of the certificates that the Client decides to include in them:
  - Personal identification information includes unique identity numbers, such as identification documents or passport number, employee number or others that the client uses to identify certificate holders
  - Professional contact information, such as professional email address
  - Professional relationship information, such as company and job position or powers granted
  - Image of the signature that may appear on documents stored on the nebulaSUITE

- The certificates themselves qualified as support for the data of the certificate holders.

- In the case of using nebulaID for remote video identification:
  - Identification data
  - Image of identity documents

- OCR processing results of identity documents
- Recorded video images of proof of life of the platform user, including voice records.
- Verification process audit records
- Data on the applicant's circumstances depends on the type of certificate to be issued (position or representation, professional registration, qualification).

Special category data:

- This ATD does not consider the processing of data classified as "special category data" or requiring special protection measures.

- The processing of such data on behalf of the client should only be carried out with prior agreement between both parties and after having carried out an appropriate data protection impact assessment prior to processing.

- In the case of using nebulaID, although a facial recognition process is carried out using biometric techniques, no biometric data is stored.

Nature of treatment

Depending on the services contracted:

- VÍNTEGRIS will process the Client Data through the Services provided by the nebulaSUITE platform.

- It involves the activities of:
  - Registration and storage of customer information
  - Deletion or destruction of information when required by the Client and upon termination of the service
  - Limitation of the processing of information at the request of the Client or competent authority.

- For services provided through nebulaID:
  - Capturing videos of users and their identification documents
  - Scanning and OCR processing of identification documents
  - Application of facial recognition algorithms, contrasting the image of the person with that contained in the identification document using documentary validation technology and facial biometrics.
  - Conservation of evidence collected during the recognition process during the periods established by legal obligations.

- All data is stored on servers in the EU using services provided by third parties as stipulated in the ANNEX IV List of Subprocessors.

- The data is provided by the Client as the data controller when using the Services.

- Processing on the nebulaSUITE platform is automated, so VÍNTEGRIS staff cannot access the Client's data. If applicable, this access would only occur under the express request and supervision of the Client, for example, in the case of requiring support for its use or resolution of a problem reported by the Client.

- VÍNTEGRIS considers that it does not have instructions to process other personal data that may circumstantially be included in the content managed by the Client.

- Any additional personal data that is processed by VÍNTEGRIS on behalf of the Client must be agreed as an amendment to this ATD.

Purpose of the processing of personal data on behalf of the data controller

Depending on the services contracted:

- VÍNTEGRIS will process the data solely to provide the contracted nebulaSUITE platform services and by the General Conditions of the Service.
- VINTEGRIS will process the data exclusively to perform identity validation through video identification.

Treatment duration

- This ATD applies for the duration of the service, as established in the nebulaSUITE service provision contract or agreement signed by both parties.

- Following the termination of the contract or agreement, VÍNTEGRIS will maintain its obligations regarding the data processed under the period determined by the data retention policy described in the nebulaSUITE General Conditions of Service or other terms expressly agreed between both parties.

- In the case of the use of nebulaID services, in accordance with the provisions of current regulations, which regulate remote video identification methods for the issuance of qualified electronic certificates:

    - A copy of the video recording will be kept for a minimum period of fifteen years from the expiration of the validity of the certificate obtained by this means.

    - Photos or screenshots of the applicant and the identity document used will be kept for a minimum of 15 years, in which both the person and the front and back of the identity document will be recognizable.
    - The automatic result of the verification carried out by the application, as well as the evaluation and observations made by the operator, together with their decision to approve or reject the identification, will be kept for a minimum period of fifteen years.

    - All evidence of incomplete identification processes that have not verified the authenticity, validity and physical and logical integrity of the identification document used and the

correspondence of the holder of the document with the applicant will be kept due to suspicion of attempted fraud during a period of 5 years from the execution of the identification process, specifying the reason why they were not completed, by the policy established for this purpose.

- The conservation will be carried out by blocking the data, in accordance with the provisions of article 32 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

ANNEX III. Technical and organisational measures to ensure data security

VÍNTEGRIS applies the necessary technical and organizational security measures to guarantee an adequate level of information security in order to protect the confidentiality of personal data, as well as to protect it against accidental or unlawful destruction or accidental loss, alteration, disclosure or unauthorized access, considering the nature, scope, context, and purpose of the processing, as well as the risks to the rights and freedoms of natural persons.

These measures are implemented under an Information Security Management System framework with the ISO 27001:2017 , 27701and 27018 certification and the National Security Scheme (ENS) certifications in the HIGH category and the compliance with eIDAS. Regulation and NIS2 as qualified trusted service providers.

On the other hand, the Client is responsible for implementing and maintaining security measures and protecting pertinent personal data as a user of the Services in those aspects that are under its control.

Consequently, VÍNTEGRIS confirms that it has implemented the measures listed below that apply to the treatments carried out on behalf of the controller.

IMPLEMENTED SECURITY CONTROLS

POLICIES OF THE ORGANIZATION	
Security policy	An information security and personal data protection policy is published and known to all staff and collaborators.
Security Manager	VÍNTEGRIS has designated a Chief Information Security Officer ("CISO") to coordinate and supervise security rules and procedures.
Security roles and responsibilities	Information security roles and responsibilities are defined and assigned appropriately within the organization. VÍNTEGRIS personnel who manage the Services that contain Client Data are subject to confidentiality obligations, information security regulations, and personal data protection regulations.
Risk management program	Within the Information Security Management System framework, there is a plan for evaluating and treating information security risks, which is reviewed periodically.

Continuous assessment	VÍNTEGRIS conducts a periodic verification and evaluation of the effectiveness of the technical and organizational measures implemented to protect information security in the processing systems, work centers and users who use them. This evaluation and review is carried out under the criteria of industry security standards and the policies and procedures determined by the Information Security Management System.
Supplier Security Policy	There is a formal process that allows assessing compliance with the information security requirements that providers who process personal information and data must meet. Suppliers are only given access to information when there is a legitimate need to justify this access.

STAFF AND COLLABORATORS	
Confidentiality Commitment	All staff and collaborators with access to personal information and data have signed a commitment regarding: ● Keep secret and guarantee the confidentiality and security of the data to which they may have access for reasons of their employment, contractual or any other type of responsibility. ● Do not use the confidential information to which they have access for purposes besides those determined. ● Do not communicate, reveal, disclose or transfer confidential information to unauthorized third parties. ● Maintain the duty of secrecy for a minimum period of 1 year once the employment or contractual relationship ends.
Internal information security regulations	There are regulations on information security, personal data protection and computer media use that all staff and collaborators have agreed to comply with.
Information Security Training	All staff and collaborators with access to personal information and data have received adequate training regarding information security and the protection of personal data.
Rules for the use of information systems	The information security regulations establish the standards for acceptable use of the information systems and equipment that the personnel are in charge of.

Prohibition of use for personal purposes of corporate equipment	It has been established that the use of those computers and devices intended for the processing of corporate information and personal data for private purposes is not permitted. Access to corporate information from private computers is also not permitted.

SAFETY AT THE WORKPLACE	
Unattended computers	A mechanism has been established so that when a computer is left unattended, the screen is locked or the session is closed.
Documentation custody	Regulations have been established so that paper documentation or information carriers are not left unguarded in the workplace at any time.
Secure destruction of information	Mechanisms have been established to facilitate the secure destruction of confidential information on paper or other electronic media.
Secure teleworking position	A policy has been established so that teleworking can be done safely.
Mobile device security	A policy has been established to protect the use of mobile devices and the information they may contain.

MANAGEMENT OF INCIDENTS AND SECURITY GAPS	
Incident management procedure	A procedure has been defined to record and resolve incidents affecting information and personal data security.
Procedure for managing security breaches in personal data	The procedure makes it possible to identify when a security breach of personal data occurs and to provide notification to the person responsible immediately and without undue delay about said security breaches, including all the information necessary to evaluate the impact and determine the causes and corrective measures applied.
Assistance to the person responsible for the notification of security breaches	It is planned to assist the controller in notifying the security breach to the supervisory authority and, where appropriate, the interested parties, considering the information available to the controller.

ACCESS TO SYSTEMS	
Access control policy	VÍNTEGRIS maintains an access control policy that determines the security privileges of the people with access to the information.
Access authorisation	There is a formal process to manage the authorization, registration, cancellation and modification of user access to the systems.
Individual accounts	Each person uses an individual, non-transferable user account.
Least Privilege	VÍNTEGRIS has defined and applies a default minimum access policy, which guarantees that staff and collaborators only have access to the information they require to perform their job duties.
Accounts with privileged access	To perform system administration and configuration tasks, nominal access accounts with privileged rights are used that are different and segregated from the accounts for ordinary use of the systems
Authentication	VÍNTEGRIS uses industry standard practices to identify and authenticate users attempting to access information systems. Two-factor authentication systems are used to access those most exposed networks or systems administration. All systems include controls to prevent repeated attempts to gain access to information systems using an invalid password. Use of MFA.
Password security	The existence of password policies (or equivalent mechanisms) will be guaranteed for access to systems and applications that comply with at least the following: ● Password length: minimum 8 characters ● Periodic password renewal ● Password complexity requirements ● Limits on password reuse

Password Confidentiality	There are regulations to ensure the confidentiality of passwords, preventing them from being exposed or shared with third parties. Internally, all passwords are saved using irreversible encryption algorithms.
Access logs	A record of access and attempted access to the systems is maintained and monitored.
INFORMATION PROCESSING ASSETS	
Actives' inventory	There is an inventory of the systems and equipment used in processing information, with the information of the person responsible for said equipment.
Safe Disposal and Reuse	Formal processes have been defined for the safe disposal and/or reuse of information processing equipment.
Equipment maintenance	The systems and equipment used to process the information are properly maintained or updated.
Malware protection	The computers on which information is processed or stored have permanently active and updated anti-malware protection.
Software update	All software used to process information is duly updated without known serious vulnerabilities.
Bastion of systems	System hardening measures have been applied, such as, among others: ● Have only the essential ports open ● Disable all services not strictly necessary ● Lock or change default passwords for accounts with privileged access ● Encryption of the disks that contain the information
Limitation on software installation by users	There are regulations or technical measures to prevent staff from installing unauthorized software on their work equipment, as well as to prevent software that may violate the intellectual property of third-parties from being used.

Limiting administration privileges	Technical measures have been implemented so that users cannot modify or deactivate the security configurations of the equipment.
Restriction on use for personal purposes	There is a regulation that prohibits the private or personal use of corporate equipment.

PROTECTION OF INFORMATION IN TRANSIT AND AT REST	
Perimeter network protection	There is perimeter protection of the network to protect it against attacks and improper access to those systems in which the storage and/or processing of information and personal data is carried out.
Network segregation	The network has been configured so that there are segregated security zones according to the different security requirements that have been established.
Secure information transmission protocols	All traffic on the organization's networks, especially when it passes in whole or in part over public networks, is encrypted using secure protocols and without known serious vulnerabilities (for example, minimum TLS 1.2
Secure remote access	For remote access to the organization's network, for example, using virtual networks (VPN), secure protocols and authentication keys of the communication ends are used.
Encryption of information on transit media	There are mechanisms to encrypt information on media and equipment in transit outside the usual processing facilities.
Vulnerability scan	Tests are periodically carried out to verify that the networks are free of vulnerabilities and that the necessary corrective measures are applied.
Wi-Fi network segregation	Wi-Fi networks for visitors are segregated so that access to the company's internal networks is not possible.

Security of cloud provider services	In the case of using services from a cloud provider (IaaS, PaaS, SaaS,...) to process the information, it is guaranteed that the provider provides or allows the application of security measures at least equivalent to those required of the person in charge.
Audit logs	Audit records of operations performed on data (access, modification, and deletion) are collected, preserved and reviewed, especially when special category data is processed.
Segregation of client instances	Segregation of services to different clients through a multi-tenant architecture. Logical segregation of users and data is provided.

PHYSICAL SECURITY OF TREATMENT SPACES	
Physical security perimeter	There is a security perimeter to protect the premises and rooms where information is processed or stored.
Access limitation	Physical access controls have been implemented at the facilities where information processing is carried out to ensure that only authorized personnel have permitted access.
Physical access control	Specific entry controls have been established to limit access to strictly authorized personnel to secure areas where servers, network equipment or document files used for the processing and storage of information are located.
Protection against external and environmental threats	The necessary measures have been established to protect people, equipment, and facilities in the event of natural disasters, malicious attacks or incidents, such as fire, floods, water leaks, air conditioning failures, etc.
Supply facilities	The necessary measures have been established to guarantee the continuity of the electrical supply.

Security of processing centre providers	The external data centers where the VÍNTEGRIS servers are located in the EU require that they must be at least TIER III and have information security certifications. More information in Annex IV, "Subprocessors"
Security of IaaS and PaaS service providers	IaaS and PaaS service providers provide the necessary physical security controls guaranteed through appropriate certifications such as ISO 27001, SOC 2, ENS (High level), PCI-DSS, and others. In this case, the services are contracted in data centers located in the EU. More information in Annex IV, "Subprocessors"

SYSTEMS RESILIENCE	
Systems Availability	VÍNTEGRIS has established measures to guarantee the availability of the systems under the committed service levels.
Monitoring and capacity management	The performance of the systems is continuously monitored, with alert systems to detect any incident immediately. Systems capacity monitoring is continually carried out to ensure the availability of sufficient capacity for the required services.
Redundancies	All Víntegris systems are redundant, internally on different servers and in different geographically distant data centers.
Backups	VÍNTEGRIS makes a backup copy stored on a medium dissociated from the usual treatment equipment. This copy is made with the necessary frequency to meet the committed service levels. Additionally, VÍNTEGRIS maintains a backup copy stored in a different location and geographically separated from the usual information processing facilities. This copy is made with the necessary frequency to meet the service levels committed in the event of a serious incident at the treatment facilities.
Backup Monitoring	The correct execution of backups is continuously monitored.
Recovery tests	Periodic recovery and verification tests are carried out on the information contained in the backup copies.

Continuity Plan	A Continuity Plan has been developed to recover the availability of the systems and the integrity of the information in the event of a serious incident.
Recovery procedures	Specific protection and recovery procedures are available against threats that compromise the integrity of the information, such as ransomware attacks.

PRIVACY BY DESIGN AND BY DEFAULT	
Minimisation of data collection	Only the data strictly necessary for the purpose for which they must be processed is collected.
Limitation of the data retention period	VÍNTEGRIS has established procedures to limit data retention and avoid its conservation beyond the established periods. Temporary files created as a result of processing are deleted when they are no longer needed.
Purpose limitation	VÍNTEGRIS has defined mechanisms to prevent the information processed on behalf of the person responsible from being used for purposes apart from those established in this Data Processing Agreement (DTA).
Pseudonymisation and data encryption	Pseudonymization and data encryption measures are applied, especially when the information processed includes data of a special or susceptible category.
Segregation of sensitive information	Access to the most sensitive information is segregated so that authorized personnel can only consult and process it.

EXERCISE OF THE RIGHTS OF INTERESTED PARTIES	
Response procedure	VÍNTEGRIS has defined a formal process to attend to and assist the person responsible for responding to requests to exercise the rights of the interested parties.

Communication of requests to exercise rights	VÍNTEGRIS has defined the channels to communicate requests to exercise the rights of the interested parties to the data controller.
Treatment limitation	There are mechanisms to limit data processing whenever required.

ANNEX IV. List of subprocessors

An agreed list of subprocessors in accordance with Clause 6.7(a), depending on the services contracted:

Name of sub-processor	Amazon Web Services Inc.
Treatment description	IaaS and PaaS service provider
Location of treatment	European Union (Ireland, Frankfurt, Paris)
Address and contact details	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855, Luxembourg Tel: +352 2789 0057
Guarantees provided	https://aws.amazon.com/compliance/gdpr-center/

Name of sub-processor	VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.
Treatment description	Provider of the technological platform on which the identity recognition process is supported the technological platform on which the identity recognition process is supported.
Location of treatment	Spain
Address and contact details	Email: partners@veridas.compartners@veridas.com
Guarantees provided	Treatment manager agreement included in the Use and Distribution License Agreement for platforms signed between Víntegris and Veridas.

When Vintegris acts as a data processor for another trusted service provider:

Name of sub-processor	AE Group S.à r.l. (AtlasEdge)
Treatment Description	Provider of the data centres where VÍNTEGRIS servers are located. AtlasEdge personnel cannot access the servers or the data contained therein.
Location of treatment	Spain (Barcelona and Madrid)
Address and contact details	Email: privacy@atlasedge.com
Guarantees provided	https://atlasedge.com/documents/AtlasEdge%20Procurement%20GTCs%20v01.09.21.pdf

	https://atlasedge.com/wp-content/uploads/2021/10/AtlasEdge_Barcelona-DC_DataSheet.pdf https://atlasedge.com/wp-content/uploads/2021/10/AtlasEdge_Madrid-DC_DataSheet.pdf