multiSign cloud

# GENERAL TERMS AND CONDITIONS

*Ver. 2 - 10/01/2022*

**Summary**

## 1 DEFINITIONS

| TERM | DEFINITION |
|---|---|
| Supplier | itAgile SRL, registered office in viale America 111, Rome, Certified E-Mail: itagile@pec.it |
| Customer | The company, or other entity, that signs a Contract subject to the General Terms and Conditions |
| Contract | The set comprising the General Terms and Conditions and all Subscription Contracts or Orders |
| Service | Means by which the Supplier can provide value, in terms of utility and warranty, to its customers by facilitating the results that customers wish to achieve |
| SLA | Service Level Agreement |
| Intellectual Property Rights | Patents, copyrights, models, trademarks, registered designs, moral rights, design rights (registered or not), know-how, databases, names and trademarks, the rights to proprietary information and data, and any other proprietary rights (including related registration requests, and the right to request registration or protection of the rights listed above), existing or applicable anywhere in the world |
| Availability | The guarantee of the minimum availability of the subscribed service, measured as a percentage based on calendar months for the duration of the service |
| Documentation | The online instructions and explanations, manuals and other written or recorded documents, including videos, and any manuals provided by the Supplier relating to the use of the Service |
| Maintenance | Maintenance, Updates, installation of new versions, and repairs to hardware and software |
| Force Majeure Events | Anything that is not reasonably predictable and controllable by one of the contracting parties, such as earthquakes, floods or other natural interventions; acts of war, hostility and sabotage; failure of the electricity, telecommunications, or Internet network, not directly caused by one of the contractors, or regulatory and binding |
| Users | Employees, managers, consultants, and in general those acting on behalf of the Customer, who receive a user code and/or password (credentials) to access the Service online |
| Update | Any modification, correction of error or improvement made to a Service Component, which the Supplier makes available to him unquestionable decision, on the basis of this Agreement |
| Third Party Software | An online Internet application, or an off-line software product, provided or licensed by third parties, and that is inter-operating with the Service (e.g., browser) |

## 2 STRUCTURE AND SUBJECT MATTER OF THE CONTRACT

This contract regulates the relationship between Supplier and Customer during the period of provision of one or more the multiSign Cloud service. The contract is implicitly signed by the Customer at the time of activation of the service. The terms of this agreement are integrated by the conditions present in any commercial and technical offer proposed by the Supplier to the Customer and by the conditions present in any contract with the Customer for specific supplies. In the event of discrepancy, the terms of this agreement shall apply where otherwise provided for in expressly. The transfer to third parties, in whole or in part, defined as the "resale" of the services covered by this Agreement is permitted without prejudice to the responsibilities and limitations set out herein. Any ancillary services requested by the Customer even after the conclusion of this agreement are subject to the same conditions and are considered a component of the service. The contractual scheme is that of the rental of things, that is, the license of use, so the customer will never acquire ownership of the services provided.

## 3 COMPLETION OF THE CONTRACT AT SERVICE ACTIVATION

The contract is finalized when the service is activated. The customer account email receive communication by e-mail about the service activation.

## 4 DURATION OF CONTRACT RENEWAL AND TERMINATION

The duration of the contract is defined in the commercial offer that the Customer subscribes at the time of sending the order to the Supplier or at the time of the request of the online service. The subscribed services, unless otherwise defined, are automatically renewed at expiration, for the same period and under the same conditions. In case of automatic renewal, the Customer can cancel the service - sending a written communication to the Supplier or opening a ticket - within 5 days before the deadline.

## 5 FEES AND METHODS OF PAYMENT

The fees are defined in the commercial offer that the Customer subscribes online or by sending the order to the Supplier. The commercial offer defines how the service is paid.

## 6 NON-PAYMENT

Failure to pay for the service determines – within the time limits and methods defined at the sole discretion of the Supplier – the suspension of the service and any cancellation. In case of suspension or cancellation, the Supplier reserves the right to ask the Customer for compensation for the restoration of the service.

## 7 OBLIGATIONS AND LIMITATIONS OF SUPPLIER LIABILITY

### 7.1 Data interoperability

8.1.1 – The Supplier will not be liable in any case for errors, nor for the loss or damage of customer data, even if the data is not managed through the Service itself, or are the result of defects in data loading processes, even if the extraction of data from the Customer's Database and/or the uploading of data into the Customer's Database have been done using interoperability tools, such as application programming interfaces (APIs) or other service or support software components that may be provided by the Supplier.

8.1.2 - The Supplier may include in the Service features that are based on interoperability with Third-Party Applications (e.g., DocuSign applications or TrustPro certificates). The availability of such applications may in the future become subject to obtaining the customer's right of access directly from the application provider. The Supplier offers no guarantee regarding the availability over time of such applications, and the Customer acknowledges that, if a supplier ceases to make a Third-Party Application available for interoperability with the Service on conditions deemed acceptable by the Supplier. The Supplier may, at its discretion, remove the corresponding function from the Service without the Customer being able to object.

### 7.2 Supplier guarantees

8.2.1 – The Supplier guarantees for the service: (i) that it has the right to license the software that constitutes the Service; (ii) that such software will work as described in the Documentation; (iii) that the Service will be provided with adequate expertise, diligence and professionalism in line with current business practice in the sector; and (iv) that the Service will be provided in compliance with the following SLA: The guaranteed level of service is 99.95% on an annual

basis. In case of exceeding this limit, the Supplier will recognize the Customer a credit equal to 1% of the cost of the annual service, for every 30 minutes exceeding the guaranteed availability threshold up to a maximum of 300 minutes.

8.2.2 – The supplier guarantees that it has the right to grant the user licenses made available to users for software provided by the Third-Party Supplier or Software in accordance with copyright

8.2.3 - The guarantees of Article 8.2.1. do not cover any deficiencies or damage due to: (i) interaction with Third Party Applications and/or with software, services or non-Supplier content; (ii) any connectivity provided by third parties; (iii) any change to the Service not made by the Provider or (iv) any operation that is different from what is indicated in the Documentation that is caused by the use of the Service in a manner that does not comply with the Terms of Use of the Cloud Services.

8.2.4 - Except for what is expressly established in this Agreement, all warranties and conditions, express or implied, provided for by law, regulations or other source are excluded to the maximum extent permitted by law or, in any event, by the remaining amount of the contract. No warranty is granted regarding the results that the Customer can obtain by the Service nor that the Service will work without interruption and without errors.

8.2.5 – The Supplier guarantees the possibility for the Customer to request 2nd Party Audits. Where there is no possibility to perform audits by the Customer, the Supplier makes available the view of the certificates obtained in accordance with the standards UNI CEI ISO/IEC 27001:2017 – ISO/IEC 27017:2015 – ISO/IEC 27018:2019.

8.2.6 - If the service is paid before activation and the service cannot be activated for technical reasons the supplier applies the "money back guarantee" policy.

### 7.3 Compensation

8.3.1 - If the Service, or part of it, becomes the subject of legal action or a breach complaint in the Supplier's opinion, the Supplier at its own expense and at its discretion may: (i) give the Customer the right to continue to use the Service or part of the Service in question; (ii) replace the Service or part of the Service in question with another service or software that does not allow the same breach; (iii) modify the Service or part of the Service in question in order to eliminate the cause of the breach; or, if none of the options listed so far are possible, (iv) terminate the Customer's contract for that element of the Service that contains the disputed party, giving 30 days of written notice, and return to the Customer any prepaid fee referred to that element for the part of the Contractual Period following the date of cancellation.

8.3.2 – The Supplier will have no commitment arising from the obligations referred to in article 8.3.1 above in cases where the dispute is based on: (i) the combination, management or use of the Service with other services or with software not provided by the Supplier, if the violation could be avoided in the absence of such combination, management or use; (ii) the use of the Service in a manner that does not comply with this Agreement, or (iii) the even partial modification of the Service made by a person other than the Supplier, if the violation could be avoided in the absence of such modification.

### 7.4 Exclusions

8.4.1 – The Supplier will have no responsibility or obligation to intervene, in the event of errors, problems or malfunctions, nor in the event of non-availability of the Service, when these result from one of the following causes: (i) violations of customer obligations arising from this Agreement; (ii) errors or omissions of Internet Service Providers; (iii) use of Third Party Applications, or "Single Sign-On" functions that the Customer or a User has installed and/or enabled to enter the Service or to interact with it, including cases of dissemination, modification or deletion of Customer Data that may result; (iv) the underestimation of cyberattacks or similar incidents; (v) any DNS issues that are not under the control of the Supplier, e.g. errors in the Customer's network or in the network of an Internet service provider; (vi) any problems or errors that occur while the Supplier is waiting for the Customer to provide useful information to correct an error or restore services; (vii) inconvenience caused by the Customer's management or operational activities regarding the Service; (viii) Force Majeure.

### 7.5 Using subcontractors

8.5.1 – The Supplier may use subcontractors in the provision of the Service. The Supplier, in order to ensure that subcontractors comply with the requirements for the security of the Supplier's information, selects the same favoring subcontractors with certifications equivalent to those of the Supplier in any way contractually reserves the possibility to verify carry out 2nd party audits, where possible, at the subcontractors themselves.

8.5.2 – The Supplier, if in the use of subcontractors transfers personal data the same will be reported within the appointment as data controller.

8.5.3 - The Supplier, in the event of a change of subcontractor, undertakes to notify the Customer of this change, before it is implemented.

### 7.6 Retention, Return and Deletion of Customer Data

8.6.1 – The Supplier guarantees the storage of Customer data throughout the period of validity of the contract according to best security practices and in compliance with the European regulation for the protection of personal data 2016/679.

8.6.2 – The supplier guarantees the safe deletion of customer data, and except for data relating to the digital signature certificate and data relating to the Supplier's tax obligations, exclusively at the explicit request of the Customer: (i) at the end of the period of validity of the contract; (ii) following termination of the contract. The safe deletion of the customer's data will take place according to the Supplier's procedures.

8.6.3 – The Supplier will periodically carry out the log monitoring activity.

### 7.7 Changes in service

8.7.1 – The Supplier, in order to improve its management, may make changes to the Service by modifying what is described in the Documentation, and/or by communicating it to the Customer by e-mail.

8.7.2 – These changes may include, for example: (i) changes in the minimum equipment configurations (such as computers) necessary to use the Service; (ii) changes to the rules of use, security and confidentiality rules, or new rules to ensure the security and integrity of the Service; (iii) amendments to the General Terms and Conditions concerning Third Party Applications and content made available by The Supplier; (iv) limits on the amount of memory space that can be used for customer data (including customer's Additional Documents), and similar restrictions aimed at avoiding unreasonable loads on the Service; and/or (v) rules to ensure that the databases and applications forming part of the Service can be used as effectively as possible and within the limits of available capacities.

### 7.8 Datacenter location

8.8.1 – The Supplier uses co-location solutions in the following datacenters:

- Aruba Spa – Arezzo
- TrustPro Ltd - Dublin
- itAgile - Rome

## 8 OBLIGATIONS AND RIGHTS OF THE CUSTOMER

### 8.1 Interoperability of data, third-party applications and suppliers

9.1.1 - If the Customer uses third-party products or services, including, but not limited to, other applications not provided by the Supplier, and/or location, configuration, consulting services provided by third parties, and/or if you exchange service-related data with a third-party provider, including in the case of use of Application Programming Interfaces (APIs) provided by the Supplier for access to Customer Data, any agreement regarding these operations is exclusively between the Customer and the third-party provider of the product or service. The Supplier does not provide any warranty or assistance on third-party products or services, even if these have been recommended by the Supplier.

9.1.2 - If the Customer installs or enables Third Party Applications or services (e.g., "web services") that can be used with the Service, the Customer requests and acknowledges that the Supplier may allow the providers of such Third-Party Applications or Services to access customer data to allow interoperability with the Service. The Supplier assumes no responsibility in cases of disclosure, modification, or loss of Customer Data because of access by Third Party Applications or service providers.

9.1.3 - In the cases indicated in the previous points of this article, the Customer must request explicit authorization from the Supplier by opening a ticket using support service at https://support.itagile.it .

### 8.2 Customer guarantees and responsibilities

9.2.1 – The Customer guarantees that he has all the rights of use, respect copyright and any related rights necessary to comply with their own obligations under this Agreement.

9.2.2 - The Customer accepts and is aware that the guarantees of Article 9.2.1 do not cover any deficiencies or damage due to: (i) interaction with Third Party Applications and/or with software, services or content not of the Supplier; (ii) any connectivity provided by third parties; (iii) any change to the Service not carried out by the Supplier; or (iv) any operation that is different from what is stated in the Documentation that is caused by the use of the Service in a manner that does not comply with the Terms of Use of cloud services.

9.2.3 - Customer agrees that except for what is expressly established in this Agreement, all warranties and conditions, express or implied, provided for by law, regulations or other source are excluded to the maximum extent permitted by law. No warranty is granted regarding the results that the Customer can obtain using the Service nor that the Service will work without interruption and without errors.

9.2.4 - The Customer will be liable for any violation of this Agreement due to actions, omissions or negligence of Users or other persons who access the Service with the Customer's access code, as if such actions, omissions or negligence had been committed by the Customer directly.

9.2.5 - The Customer guarantees to have all rights of use, to respect copyright and any related rights, necessary for the use of any type of software used in the cloud environment.

9.2.6 - Customer ensures that the licenses provided by Supplier are used within the limits provided by the supply.

### 8.3 Compensation

Customer will compensate the Supplier and its employees, subcontractors and those acting on its behalf all costs, losses, expenses and compensation due to third parties, including reasonable legal expenses, arising from disputes related to or resulting directly or indirectly from: (i) violations by the Customer or a User of any Intellectual Property Right in connection with the use of the Service made outside of the provisions of this Agreement; (ii) the processing by the Data Provider, including personal data, of the Customer, of other elements of the Customer or provided by the Customer, including, among other things, the storage or publication on the Internet of data or content that is defamatory, or that represents violations of Intellectual Property Rights or rights of third parties; (iii) violations of laws or other data protection legislation, including personal data protection, resulting from the processing of the data themselves carried out by the Supplier on behalf of and in accordance with the instructions received from the Customer or Users; or (iv) non-compliance with this Agreement by the Customer or a User. In addition, the Supplier will have the right to take measures to prevent the publication on the Internet of data, including personal data, or content prohibited by law, and to prevent the continuation of violations of the rights of third parties.

### 8.4 Information security

9.4.1 Customer will maintain appropriate security measures to ensure that access to the Service remains within the limits of the provisions of this Agreement. In particular, the Customer must: (i) manage with due diligence and attention any identification, password, username or other security devices for the use of the Service; (ii) take the necessary measures to ensure their confidentiality, security and correctness of use, and to prevent unauthorized persons from being in possession of them; and (iii) ensure that each user account is used only by the User to whom it has been assigned. The Customer is responsible for all activities carried out through the access keys to the Service assigned to the Customer and Users and undertakes to inform the Supplier promptly when he becomes aware of unauthorized uses of the Service or other security breaches.

9.4.2 - The Customer, following an information security incident, will have to request intervention through ticket opening (https://support.itagile.it).

9.4.3 - The Customer undertakes not to disclose or make available to third parties the confidential information known or managed in relation to the execution and/or application of the contract in the absence of specific written consent of the Supplier.

### 8.5 Customer's obligations

9.5.1 The Customer will have the following obligations: (i) prevent interference by Users or third parties with the Service; (ii) ensure that the Customer's systems are properly configured and kept up to date for use of the Service, and that they have adequate access to the Internet; (iii) promptly inform the Supplier in a timely and detailed manner in the event of problems with the Service and in the case of changes in the contacts designated by the Customer; (iv)

use and maintain effective and up-to-date software for the search, detection and removal of malware and similar threats; and (v) carry out all administrative activities of human resources related to the Service, and other activities of customer competence, including, for example: the creation, removal and management of access keys (user accounts) created after the initial preparation of the Service; the operational use of the Service by its users alone; (vi) the assurance that any access keys made available to third-party suppliers are immediately deactivated at the conclusion of their services to the Customer; (vii) the execution of data loading operations and other operations and management processes related to customer data (including all data and related changes, their validation, and the revision of the data and related changes); (viii)the analysis of the causes of error messages generated by data interfaces, and the possible correction of customer data; and the development and implementation of adequate safety standards, procedures, authorizations and controls in relation to the customer's use of the Service.

## 9 SUPPORT AND MAINTENANCE

10.1 – The Supplier regularly monitors the performances of the service with automatic tools and qualified personnel.

10.2 - Emergency maintenance. The Supplier, if possible, will notify the Customer by e-mail with at least 2 working hours' notice before performing emergency maintenance (e.g., maintenance, updates, repairs to the hardware and software aimed at the immediate solution of problems that cause instability in the Service). However, if necessary, the work may begin at any time and continue until it is complete if, the operation does not cause significant degradation to the specific environment of the Customer, and/or is otherwise necessary or appropriate for the overall maintenance or improvement of the functionality, safety or performance of the Service. The Supplier will take all necessary measures to minimize the impact on the service provided to the customer during emergency maintenance activities.

10.4 - Updates. The Supplier may, at its discretion, apply periodic updates to the Service to improve its functionality, security and/or performance. When the Supplier makes new Service Components available, the Customer will be free to choose whether to acquire new products based on the Fees or tariffs of the Contractual Fees proposed by the Supplier if they become available.

10.5 - Support services. The Supplier will make available to the Customer the standard assistance services in relation to the maintenance and operation of the Service. The Provider will provide support services via ticketing system (https://support.itagile.it); support policies include the indication of response times based on the different levels of severity of requests, and related "escalation" procedures. Requests from the Customer that are outside the scope of standard assistance services may be provided, if agreed between the Customer and the Supplier, as professional services.

10.6 - Professional Services. Any Professional Services that the Supplier may provide to the Customer, on request, are provided as a service separate from the provision of the Service or a Component, at the rates agreed between the parties. Whether ordered in conjunction with the Service Contract or separately, Professional Services are considered outside the scope of this Agreement and any disagreement or dispute regarding Professional Services does not affect the rights and obligations of the arising from this Agreement about the provision and use of the Service.

## 10 SUSPENSION OF SERVICE

The Supplier reserves the right to suspend the service in the event of customer non-compliance or due to force majeure.

## 11 EXPRESS TERMINATION CLAUSE – RESOLUTION FOR NON-COMPLIANCE – TERMINATION CONDITIONS

The Supplier reserves the right to terminate the contract in the event of customer default on any element of this contract, and/or if expressly provided for in the offer or specific ancillary contracts to the Customer's order.

## 12 WITHDRAWAL

The Customer may exercise withdrawal from the contract only if expressly provided for in the commercial offer or in contracts ancillary to the Customer's order. The Customer remains obliged for the duration of the contract unless otherwise provided for in the offer or ancillary contracts.

## 13 CHANGES TO THE SUPPLIER'S CONTRACT AND/OR POLICIES

Any change to this agreement shall be in written form and signed by the parties electronically. There is no obligation to communicate changes to the Supplier's policies if these changes do not affect the services provided.

## 14 COPYRIGHT AND LICENSING

All components of the service covered by the contract remain the exclusive intellectual property of the Supplier and its possible subcontractors. The Supplier guarantees that the service provided is free from copyright and third-party licenses that may in any way affect the Customer.

## 15 INFORMATION SECURITY

16.1 - The Supplier may suspend access to the service or to part of it if, at the discretion of the Supplier to be exercised reasonably, there is a risk that actions by the Customer or a User will compromise the integrity or security of the Service.

16.2 - The Supplier ensures the segregation of the networks between its network and that of the subcontractors.

16.3 - The Supplier will report information security incidents to the Customer through the use of the main contact provided by the Customer. The reports to the Customer of information security incidents will take place within 48 hours from the moment the Supplier becomes aware of them including in the communications the actions taken by the Supplier and/or any actions necessary for the resolution of the incident by the Customer.

16.4 - The Supplier in the use of subcontractors in the partial or total supply of the Service will notify the Customer of any information security incidents that have occurred at the supplier through the use of the main contact provided by the Customer.

16.5 - The Supplier constantly carries out control activities for the detection of any technical vulnerabilities in accordance with the controls provided by Uni CEI EN ISO/IEC 27001:2017 for the Cloud services provided.

## 16 FINAL PROVISIONS

This Agreement is written in Italian and the Italian text is the only one that will be authentic, even if, for the convenience of the Parties, the contract has been translated into other languages.

## 17 COMPLAINTS

Complaints must be communicated in advance to the Supplier through the opening of a support request (ticket) in the manner provided for in this contract.

## 18 PROCESSING OF PERSONAL DATA

19.1 - Each party undertakes to comply with the obligations arising from the applicable legislation on the protection of personal data with reference to EU Regulation 2016/679 of 27 April 2016 (GDPR) and Italian legislative decree of 10 August 2018 n. 101.

19.2 - To the extent that personal data is processed during the use of the Service, the parties agree that the Supplier acts as data processor appointed by the Customer acting as data controller of the data. To this end, the parties undertake to comply with their legal obligations regarding the protection of personal data (Ref. 19.1). The Supplier will process and retain such personal data only in the name and on behalf of the Customer.

19.3 - Customer data will be processed exclusively for the purposes of the Service provided by the Supplier and for multiSign Cloud services update or new service availability information.

19.4 - The Customer is required to ensure and guarantees that the personal data communicated and/or provided to the Supplier have been obtained in accordance with the applicable legislation on the subject (Ref. 19.1). The Customer undertakes to obtain any necessary consent of the persons whose data are processed and to make any necessary registrations with the competent authorities to allow the Supplier to transfer personal data to third parties in order to allow the supplier to fulfill its obligations under this Agreement.

19.5 - If a third party declares any violation of its rights with regard to the protection of personal data related to the conduct of the services provided for in the Contract, the Supplier will have the right to take any measures that it deems necessary to prevent such violation from continuing.

19.6 - The Supplier expressly declares that: (i) acts exclusively as data processor; (ii) adopt, like its suppliers and hosting entities, appropriate technical and organizational security measures for the protection of personal data; (iii) disclaims all responsibility in the case of processing of personal data by the Customer that do not comply with the legislation referred to in Ref. (19.1), with non-exclusive reference to the lawfulness of the processing, the correct information and consent, the exercise of the rights of the data subjects, etc.

19.7 - If the Supplier receives a request from law enforcement to disclose the customer's personal data, unless expressly prohibited by law, the disclosure of personal data will be promptly communicated to the main contact of the same. In any case, any disclosure of personal data that is not legally binding will be refused.

19.8 - The Supplier has appointed internally a personal data protection officer dedicated to managing all aspects related to privacy and which constitutes the point of contact for the processing of personal data; can be contacted using support service.

19.9 - The Supplier will promptly notify the customer of security incidents or unauthorized access to the customer's personal data (Data Breach), even if it receives such notification from the subcontractor, through the use of the main contact provided by the same. All the information provided for in EU Regulation 2016/679 of 27 April 2016 (GDPR) will be provided.

## 19 APPLICABLE LAW AND COMPETENT COURT

The supply relationship is governed by the laws of the Italian state. Any dispute arising out of – or linked to – this agreement, including those relating to its validity, interpretation, execution or resolution, must first be subject to mediation proceedings at the Italian National Institute for Mediation and Arbitration. In case of litigation, the only language of the proceedings will be Italian. In any case, the parties recognize the exclusive and subsidiary competence of the Roma (IT) court.

## 20 APPOINTMENT AS DATA CONTROLLER

The personal data provided by the Customer to the Supplier are not sensitive data and are protected by EU Regulation 2016/679 (GDPR). The customer consents to the use of personal data by itAgile exclusively for the purpose of executing this contract.

## 21 TECHNICAL MEASURES

Here are the technical measures taken by the Data Protection Provider processed in cloud services.

### *21.1* Firewall

Personal data is protected against the risk of intrusion through firewall systems, kept up to date in relation to the best available technologies.

### 21.2 Malware protection

Systems are protected against malware by using anti-malware that are kept up to date.

### 21.3 Authentication credentials

The systems are configured in a way that allows access only to subjects with unique authentication credentials (username, password and OTP).

### 21.4 Password

The password has the following basic characteristics: obligation to change on first access, minimum length 8 characters, complexity rules, expiration, history, contextual evaluation of robustness, hash storage.

### 21.5 Logging

The systems are configured in a way that allows the tracking of accesses and, where appropriate, of the activities carried out in charge of the different types of users and protected by adequate security measures that guarantee their integrity, confidentiality and availability. The Supplier, if requested, makes available to customers the logs of the applications produced by them in the use of the data services relating only to the applicant.

### 21.6 Backup & Restore

Appropriate measures are taken to ensure the restoration of access to data in case of damage to data or electronic tools. A business continuity and disaster recovery plan is put in place; they ensure availability and access to systems even in the event of major adverse events.

### 21.7 Vulnerability Assessment & Penetration Test

The Supplier periodically carries out activities of analysis of technical vulnerabilities and detects the state of exposure to known vulnerabilities, both in relation to infrastructure and application areas. Where deemed appropriate in relation to the identified potential risks, such verifications are periodically integrated with Penetration Test, through intrusion simulations using different attack scenarios. The results of the checks are regularly and thoroughly examined to identify and implement the necessary improvements to ensure the expected level of safety.

### 21.8 System Administrators

About all users who operate as System Administrators, whose assigned functions are appropriately defined in specific acts of appointment, a log management system is managed aimed at the timely tracking of the activities carried out and the storage of such data in unalterable ways suitable to allow ex post monitoring.

### 21.9 Data Center

Physical access to the Data Center is limited to authorized parties only. For details of the security measures taken with reference to the data center services provided by the subcontractor, reference is made to the security measures described by them and made available on the relevant institutional sites.

### 21.10 Communications Security

As far as its competence is, secure communication protocols are adopted by the Supplier and in line with what the technology makes available. Data flows to and from exposed cloud systems on the internet are protected using a secure TLS channel to ensure:

- Server authentication (2048-bit RSA key)
- Session encryption with symmetric encryption algorithm, considered reasonably secure on the date, with a session key of at least 128 bits

### 21.11 Encryption

The Supplier adopts the latest generation encryption techniques on the data in the databases in order to make them unusable to those who are not authorized to view them. Encryption is also applied in communications to and from supplier systems.

### 21.12 Hardening

Special hardening activities are in place to prevent the occurrence of adverse events by minimizing the architectural weaknesses of operating systems, applications and network equipment.

### 21.13 Secure erasure of temporary data and files

The Supplier ensures that the disk space made available to customers is cleaned before use through a secure erasure procedure performed at the end of the service.

### 21.14 Clock Synchronization

All cloud systems of the vendor use the NTP protocol for clock synchronization. The source of the clock is INRIM (www.inrim.it). The time zone used is CEST.

### 21.15 Secure development

The software development environment is accessible only to coding and testing personnel. The Supplier's development process follows safe development guidelines aimed at ensuring compliance with the principles of Security by Design. Code testing follows a predefined process to evaluate both the functionality of your code and the presence of serious vulnerabilities. The transition to production takes place manually and the changes are properly traced. Development, testing, and production environments are logically separate.

## 22 ORGANIZATIONAL MEASURES

Below are the organizational measures taken by the Data Protection Provider processed in cloud services.

### 22.1 Policies and regulations

The Supplier applies regulations that all users with access to information systems have an obligation to comply with and that are aimed at ensuring behaviors suitable to ensure data protection in the use of IT resources.

### 22.2 Logical access

The Supplier defines the access profiles in compliance with the *least privilege principles and* the *need to know necessary for* the execution of the assigned tasks. These profiles are subject to periodic checks.

### 22.3 Management of assistance operations

The assistance operations guarantee the execution of only the activities provided for contractually to prevent the excessive processing of personal data whose ownership is the responsibility of the Customer or the End User.

### 22.4 Incident Management

The Supplier has carried out a specific procedure for the management of IT incidents in order to ensure the restoration of normal service operations in the shortest possible time, ensuring the maintenance of service levels.

### 22.5 Data Breach Management

The Supplier has implemented a procedure, related to incident management, dedicated to the management of personal data breaches. This defines roles and responsibilities, the timing and methods of notification to the data subject and the supervisory authority.

### 22.6 Training

The Supplier periodically provides its employees involved in the management of services with courses on information security and the correct management of personal data.

### 22.7 Change Management

The Supplier has a specific change management procedure in place in view of the introduction of any technological innovations or changes in its approach and organizational structure.

### 22.8 Internal audit

The Supplier assigns to qualified external personnel the execution of internal audits on the security of quality information, business continuity and privacy; the frequency of these activities is specified in the annual audit program.

### 22.9 Certifications

the Supplier has obtained certifications for the field of application "provision and management of remote digital signature services" according to the following international standards:

- UNI CEI EN ISO/IEC 27001:2017
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- UNI EN ISO 9001:2015

## 23 LIMITATIONS ON THE USE OF THE SERVICE

Failure to comply with the following conditions will result in the immediate suspension of supply. For any requests for clarification regarding the General Terms and Conditions the customer can open a ticket at the address https://support.itagile.it

### 23.1 Violations

The use of the remote signature service for illegal activities, in the sole opinion of the Supplier, results in the termination of the service. The credentials to access the service are strictly personal and not transferable to third parties. The following is an example of prohibited activities:

- Transfer of login credentials to third parties
- Unauthorized access (or use)
- Denial of service
- Load test

### 23.2 Vulnerability Test

It is necessary to agree with the supplier any Vulnerability Assessment and Penetration Test activities. Execution without written consent may result, at the discretion of the Supplier, in the termination of the service.