GENERAL TERMS AND CONDITIONS FOR THE PROVISION OF SERVICES AND SOFTWARE

1. Definitions

The Parties agree that, unless otherwise defined elsewhere and not expressly mentioned here, the terms listed in the Contract are assigned the following meanings:

a) **Data Processing Agreement**: the agreement in accordance with Article 28 of EU Regulation 2016/679 (known as the "General Data Protection Regulation" or "GDPR");
b) **Client**: the natural or legal person who, by signing the Contract, acquires the right to use the Services and Software offered by Namirial, if applicable also through the Partner;
c) **Additional Conditions**: the contractual conditions, additional and specific to the General Conditions, applicable to one or more of the Services and Software identified in the Commercial Proposal;
d) **General Conditions**: these general terms and conditions of the contract;
e) **Specific Conditions**: the contractual conditions, additional and specific to the General Conditions and the Additional Conditions, applicable to one or more of the Services and Software identified in the Commercial Proposal;
f) **Contract**: the set of contractual documents (Commercial Proposal, General Conditions, Additional Conditions, and Data Processing Agreement) that define the mutual rights, obligations, and responsibilities of the Parties, necessary for the activation of one or more Services and Software offered by the Namirial Group;
g) **Technical Documentation:** a technical document and/or product specification providing a detailed description of the Software and Services, where applicable attached to the Contract and/or accessible online on the website indicated in the Contract;
h) **Namirial Group**: the group of companies headed by Namirial S.p.A.;
i) **Namirial**: Namirial S.p.A., the parent company of a group of companies offering professional management tools, digitization services, remote identification and *onboarding* of users, and the issuance of qualified electronic signature certificates;
j) **Parties**: Namirial, the Client, and, if present, the Partner, collectively;
k) **Partner**: the commercial operator who resells to the final Client the Services and Software offered by the Namirial Group;
l) **Commercial Proposal**: the contractual document that identifies the Services and Software subject to the Contract, and defines its duration and economic conditions;
m) **Connected Services**: services connected to the use of applications and other IT resources, such as, for example, the assistance service or the ordinary software maintenance service;
n) **Services and Software**: the Services and Software offered by the Namirial Group, as per Article 2 of these General Conditions, identified in the Commercial Proposal and possibly governed by Additional Conditions;
o) **Service**: may consist of providing the Client with functionalities or other utilities (e.g., remote identification of the user or the issuance of a qualified electronic signature certificate), which the Client uses within its own *business* without directly having the software tools necessary for the provision of the Service;
p) **Software**: an IT application, owned by the Namirial Group and/or its respective Sub-suppliers, made accessible to the Client in *on-premise* mode (installed at the Client's infrastructure) or *SaaS* mode (provided through the Namirial Group's infrastructure);
q) **Sub-suppliers**: companies that provide, in whole or in part, the Services and Software subject to the Contract;
r) **Users:** the end users of the Client.

The terms indicated in the definitions are always used with a capital letter, both in the singular and plural.

2. Services and Software of the Namirial Group

These General Conditions apply to the Services and Software of the Namirial Group subject to the Commercial Proposal, relating, among others, to the following areas:

a) Software for the construction industry.

The Services and Software are made available to the Client for professional use.

3. Conclusion of the Contract

The Contract is considered concluded upon signature of the Commercial Proposal by the Client, to which are attached:

a. these General Conditions;
b. the Additional Conditions;
c. any Specific Conditions
d. the Technical Documentation;
e. the Data Processing Agreement;
f. any technical documentation and/or product specifications.

The Client acknowledges and accepts that access to the Services and Software and their use entails, in any case, acceptance of these General Conditions.

Any signing of the Data Processing Agreement is separate and takes place simultaneously with the signing of the specific Commercial Proposal.

These General Conditions apply to the Services and Software subject to the Commercial Proposal, as applicable and unless otherwise provided in the Additional Conditions. In the event of conflict between the provisions of these General Conditions and those set out in any annex to the Contract, the latter will prevail in relation to the specific Service or Software for which they are established, in the following order:

- Commercial Proposal;
- Specific Conditions;
- Additional Conditions;
- General Conditions.

4. Object

The Contract may cover the provision of one or more Services and Software, also in combination with each other, as specifically identified in the Commercial Proposal.
The provision allows the Client to use the Services and Software within the limits and under the conditions indicated by this Contract.
When the activation of the Services and Software involves making IT applications available to the Client, Namirial, also through the Partner, shall also guarantee the provision of any Connected Services, whose characteristics are indicated in the Additional Conditions. It remains understood that these General Conditions apply, as compatible, to all Connected Services.
Unless otherwise specified in the Additional Conditions, the Services and Software are provided "AS IS" and "AS AVAILABLE". The Client, therefore, by signing the Commercial Proposal, declares that the Services and Software subject to the Contract meet and are suitable for the purpose for which they are purchased and that they satisfy the technical and functional requirements necessary for that purpose.

5. Activation and Access to Services

The activation of the Services and Software takes place according to the methods and timelines defined in the Commercial Proposal.
Services distributed online are made accessible upon creation and configuration of the user profiles enabled to access them and issuance of the related authentication credentials.
Through specific functionalities, if provided, the Client may create and configure additional user profiles beyond those created during activation of the Service.
Access to the activated Services and Software is permitted exclusively to the Client; therefore, the Client is prohibited from transferring the authentication credentials to third parties without the prior express authorization of Namirial.

6. Economic Conditions, Invoicing and Adjustment of Fees

The economic conditions are defined in the Commercial Proposal or in subsequent contractual documents amending or supplementing it. Where a discount is provided, it applies exclusively to the initial fees paid in advance by the Client and is entirely removed in relation to subsequent fees, unless the Parties agree on the application of a new discount.
Unless otherwise indicated in the Commercial Proposal, Namirial shall issue an invoice for the full annual amount due for the Services and Software, in advance and on an annual basis. The Client undertakes to settle the invoice amount within thirty (30) days from the end of the month of the invoice date. Payment shall be made by bank transfer to the account details indicated in the invoice.
The invoice shall be issued on the date of signing of this Contract, and in any case no later than thirty (30) days from that date, without any further documentation being required (e.g., any purchase order).
The Client may purchase additional services to be used within the scope of the Services and Software. The purchase of such services is subject to the existence of a valid licence for the use of the relevant Service and/or Software, whether granted under the same Commercial Proposal or a different Commercial Proposal previously signed by the Client. Such services are available exclusively for use within the relevant Service and/or Software and must be consumed within the term of the Contract or, in case of renewal, within the corresponding renewal period. Unless otherwise expressly provided in the applicable Commercial Proposal, any such services not used by the expiry of the relevant contractual period – whether the initial term or a subsequent renewal – shall automatically lapse and shall not be transferred or carried over to any subsequent period.
The Client acknowledges and accepts that, starting from:

- the second (2nd) year of validity of the Contract, in the case of a fee in the form of an annual prepaid charge; or
- 1 January of the year following the year of signature, in the case of a pro-rata fee,

the amounts due by the Client may be subject to an annual adjustment up to the higher of: the variation of the ISTAT Consumer Price Index for the Whole Nation (NIC) recorded with reference to the month in which the increase is applied, plus 3 (three) fixed percentage points, or 5 (five) percent of the total amounts due by the Client for the relevant period. Such adjustment will be reflected in the relevant invoice; it being understood that Namirial reserves the right to apply such adjustment also at a later time. Adjustments following the first one will be made on the price already previously adjusted.
In the event of a sale through a Partner, the economic conditions proposed by the Partner shall apply.

7. Namirial's Obligations and Guarantees

Namirial is obliged to allow the Client access to the Services and use of the Software in accordance with the technical specifications defined in the Commercial Proposal and/or the Additional Conditions, in compliance with the service levels possibly agreed and formalized by the Parties.
Namirial undertakes to make every reasonable effort to ensure the maximum availability of the Services and Software without discontinuity or interruption, except for the legitimate causes of suspension under Article 10.
To the extent permitted by law, Namirial disclaims any express or implied warranty, including the implied warranties of non-infringement, merchantability, and fitness for a particular purpose.
Unless otherwise provided in the Additional Conditions, and subject in any case to the statutory obligations applicable to specific types of Services and Software, in cases where the Services and Software are provided "AS IS" and "AS AVAILABLE", Namirial does not guarantee that:

a. the Services and Software will meet the Client's requirements and will be constantly available, uninterrupted, timely, secure, and error-free;
b. the results potentially obtainable from the use of the Services and Software will be effective, accurate, and reliable;
c. the quality of the Services and Software will meet the Client's expectations;
d. any errors or defects in the Services and Software will be corrected, unless they prevent the normal use of the Services and Software.

Without prejudice to the warranty exclusions indicated above, for any Service or Software whose compliance is required by applicable law, Namirial guarantees the compliance of the relevant Service with the technical standards in force and applicable to it, as well as with the state of the art.
Namirial uses physical, electronic, and managerial procedures to safeguard and prevent unauthorized access to the Services and Software made available to the Client. Namirial chooses these safeguards on the basis of current regulatory obligations, the sensitivity of the information collected, processed, and stored, and the current state of technology. Namirial adopts, also in accordance with the certifications it holds, all measures suitable

to ensure the security of the Services and Software, it being understood that Namirial cannot be held liable for any malicious attacks resulting from facts or conduct outside its own sphere of control or from the Client's failure to comply with its own obligations.
Namirial guarantees that it holds the certifications and authorizations necessary for the provision of the Services and Software, freely available for consultation and download on the website . This guarantee is also extended to its Sub-suppliers.https://www.namirial.com/it/company/certificazioni/
Namirial also declares that it has taken out appropriate insurance coverage, freely available for consultation and download on the website .hhttps://www.namirial.com/it/documentazione/
It is understood that if, through the use of the Services and Software, it is possible to purchase/activate third-party services, such services will be subject to the contractual conditions prepared for that purpose by the service provider. Namirial will not be liable in any way for the provision of such services.

8. Client's Obligations

The Client is obliged to promptly pay the fees due to Namirial or, if present, to the Partner for the execution of the Service and/or the supply of the Software under Article 6. In case of late payment of the fee due within the agreed terms, the Client shall owe Namirial or, if present, the Partner, from the due date, default interest at the rate set out in Article 5 of Legislative Decree No. 231 of 9 October 2002, as amended by Legislative Decree No. 192 of 9 November 2012. In addition, the Client is required to pay any costs or fees incurred by Namirial in connection with unpaid amounts, without prejudice to any other action Namirial may take against the Client in this regard, such as the suspension of the Services and Software until the outstanding payments have been settled.
The Client may not use the Services and Software for illegal purposes or in any way contrary to the provisions of this Contract. The Client is also required to ensure that its employees, collaborators, and appointees comply with the rules of use of the Services and Software under Article 9, as well as the additional specific rules contained in the Additional Conditions, the Specific Conditions – where applicable – or the Technical Documentation possibly provided (e.g., user manuals).
The Client remains fully responsible for creating any accounts or authorization profiles relating to the Services and Software, and in particular undertakes to authorize or enable only adult users.
Namirial grants the Client permission to view, copy, distribute, and download the content and materials from the Services and Software, provided that the Client:

i. retains all copyright notices and/or other intellectual and industrial property notices on the content and materials;
ii. uses them exclusively for personal or commercial purposes;
iii. does not modify them in any way.

In the case of assistance requests, the Client, where necessary, is required to allow Namirial's appointees or, if present, the Partner, access to its systems as necessary to carry out the assistance activities.
The Client is responsible for independently obtaining the necessary hardware and software tools, as well as adequate connectivity, in order to access and use the Services and Software offered, in accordance with the hardware, software, and connectivity requirements declared by Namirial in the Contract and/or in the technical documentation made available. The Client is also obliged to keep all resources necessary for the correct use of the Services and Software, including the network infrastructure, always updated and adequate. The Client undertakes to possess and maintain the technical knowledge necessary to ensure the correct use of the Services and Software offered.
The Client undertakes to respect the IP Rights of Namirial or third parties in accordance with the provisions of Article 18.
The Client acknowledges that the provision of the Services and Software may be affected by changes in applicable law or other laws, regulations, technical standards, or measures or orders issued by a competent public authority. Consequently, where such a change affects, or may affect, the Services and Software or the manner in which they are provided, the Client undertakes to cooperate with Namirial – where applicable, also through the Partner – in good faith and in a timely manner, in order to allow the continued and compliant provision of the Services and Software. Such cooperation includes, by way of example but not limited to: (i) providing Namirial with the information, documentation, and assistance reasonably requested; (ii) implementing, on its own systems and within the terms communicated by Namirial, the technical, organizational, or contractual measures, updates, or adjustments necessary to ensure compliance; and (iii) signing any amendment to the Contract or further document that may be necessary for this purpose under Article 13. Should the Client fail to provide the cooperation required under this article, Namirial – where applicable, also through the Partner – shall not be liable for any resulting unavailability, interruption, suspension, or non-compliance of the Services and Software, without prejudice to Namirial's rights under the articles on Suspension and Termination.

9. Rules of Use of the Services and Software

The Parties acknowledge that, for the correct performance of the obligations arising from the Contract, it is necessary that the conduct of both be based on full cooperation and good faith and, therefore, undertake to promptly notify each other of any circumstance that may affect the regular provision of the Services and Software subject to the Contract.
The use of the Services and Software by the Client must take place in accordance with the rules of ordinary diligence and in compliance with this Contract.
The Client may not misuse any part or content of the Services and Software. By way of example but not limited to, the Client is prohibited from:

a. making false statements, misrepresenting, or concealing its affiliation with another person or entity;
b. copying, modifying, hosting, sublicensing, or reselling the Services and Software or their content, except as provided under Article 8 above;
c. decompiling, including through a disassembler, performing reverse engineering, or attempting to derive the source code from Namirial and/or the Sub-suppliers;
d. enabling or allowing others to use the Services and Software or their content, using the Client's own account information;
e. accessing or attempting to access the Services and Software in any way other than through the interface provided or authorized by Namirial;
f. circumventing access or usage restrictions put in place to prevent certain uses of the Services and Software;
g. sharing content or engaging in conduct that infringes the intellectual property of third parties;
h. attempting to disable, compromise, or destroy the Services and Software or hardware components;
i. misusing the server infrastructure or the APIs.

The Client is also not permitted to use the Services and Software to engage in illegal, abusive, or irresponsible conduct, including:

a) carrying out any unauthorized access to, or unauthorized use of, data, systems, networks, or infrastructure of Namirial and/or the Sub-suppliers, including any attempt to probe their vulnerability, including through penetration tests, where such activities have not been previously authorized by Namirial;

b) engaging in activities that interfere with the use of the Services and Software by other users, or that cause harm to other internet users, such as, by way of example, cyber-attacks of any kind, the spreading of computer viruses or other harmful components, falsification of network packet headers, or deliberate attempts to overload a transmission system;
c) creating dangerous situations, or instability or technical problems as a result of methods of use that affect the quality of the Services and Software towards other Clients, causing harm to them, to Namirial, to the Sub-suppliers, or to third parties;
d) collecting and/or using third-party information without the consent of the owner of the information or of the data subject;
e) collecting and/or unlawfully using personal data, including e-mail addresses, names, or other identifiers (for example, spamming, phishing, internet scams, password theft, spidering);
f) disseminating any false, misleading, or deceptive information;
g) distributing software that fraudulently collects or transmits information about a user, as well as distributing so-called "adware" software, unless the user's explicit consent to the download and installation of the software has been obtained on the basis of a clear and clearly visible notice about the nature of the software;
h) offering anonymous communication systems without adequate identity retention as required by current legislation (such as, by way of example but not limited to, so-called "TOR" or anonymizers).

The inclusion, in a black-list (abuse database) such as, for example, the one available at , of the public IP addresses assigned to the Client and/or to the users authorized to access the Services and Software constitutes an automatic violation of the service usage rules under this article.www.spamhaus.org

In the event of a violation of these usage rules, Namirial, if present also through the Partner, is authorized to unilaterally adopt any measure it deems most appropriate, including the suspension of the Service under Article 10.

The Client accepts that any use of the Services and Software in violation of the rules under this article will be attributed to the exclusive liability of the Client, even where such violations are carried out by third parties using the resources assigned to the Client without the Client's consent, by exploiting passwords lost by the Client or that are insecure, vulnerabilities of software packages installed by the Client, or unlawful conduct of its employees and collaborators.

10. Suspension

Namirial, if present also through the Partner, has the right to unilaterally suspend the provision of the Services and Software when necessary:

a) to carry out technical interventions aimed at ensuring or improving the provision of the same Services and Software, provided that they are scheduled so as to ensure minimal impact on the Services and Software;
b) in the event of security risks, breaches of law, or non-compliant use;
c) to comply with statutory obligations or requests from public authorities.

In such cases, any suspensions will be communicated according to the methods defined in Article 16; Namirial undertakes to make every reasonable effort to restore the Services and Software as soon as possible.

Namirial, if present also through the Partner, also reserves the right to unilaterally suspend the provision of the Services and Software, even without notice, in the event of a violation of the obligations provided in Article 8, the usage rules provided in Article 9, and/or the policies and procedures indicated in Article 21. Namirial shall give the Client prior written notice of the violation, and the suspension may take effect only if the Client has not remedied such violation within ten (10) days of receipt of the notice. In such cases, the suspension may concern all the Services and Software subject to the Contract, even where the violation relates to only one of such Services and Software. It remains understood that Namirial shall have the right to suspend the provision of the Services and Software should the Partner fail to comply with its payment obligations towards Namirial.

The suspension may continue for as long as the relevant causes of suspension persist. Once the legitimate cause of suspension has ceased, Namirial, if present also through the Partner, undertakes to restore the availability of the Services and Software as soon as possible.

The suspension may concern all or part of the Services and Software subject to the Contract.

Namirial's right, or, if present, the Partner's right, to terminate the Contract under Article 15 and to claim compensation for any damage thereby caused remains unaffected.

11. Liability

Namirial undertakes to provide the Services and Software subject to the Contract with adequate specialization, professionalism, care, and diligence, assuming full, direct, and exclusive liability for the correct performance limited to the obligations imposed on it under the Contract. Namirial shall not be liable in any way for delays, errors, or non-performance attributable to third parties, or for anomalies that may occur during the provision of the Services and Software that are beyond its technical control, such as, by way of example only and not limited to, malfunctions in the management of telephone and/or telematic networks.

The Client is fully liable for the activities carried out using the Services and Software offered by Namirial and, therefore, any contractual or extra-contractual liability of Namirial for direct or indirect damages suffered by the Client and/or third parties as a result of the performance of the Contract is excluded, unless it is proven that the damage is attributable to wilful misconduct or gross negligence on the part of Namirial. Any contractual or extra-contractual liability of Namirial for direct or indirect damages suffered by the Client and/or third parties as a result of the Client's failure to comply with the obligations imposed on it by the Contract and by applicable law is equally excluded.

Namirial assumes no liability for any damages arising from (i) the negligence of the Client or the User and/or (ii) fraudulent action by third parties (including hacking, identity theft, etc.), unless such fraudulent action results directly from Namirial's failure to comply with its obligations under applicable laws or regulations or under this Contract.

Notwithstanding the above, it is understood that the maximum liability that each Party may bear as a result of any compensation claims made by the other Party in relation to the Contract, for damages of any nature, whether contractual or extra-contractual, will be limited to the actual damage (with express exclusion of loss of profit and damage from loss of opportunity/chances) and, in any case, will not exceed, in total:

a) for the first year, the fee paid (or accrued, in the case of a fee based on actual consumption) by the Client up to the occurrence of the non-performance;
b) for the years following the first, the fee paid (or accrued, in the case of a fee based on actual consumption) by the Client in the year preceding the one in which the non-performance occurred.

The above limitation does not apply in the event of wilful misconduct or gross negligence of the defaulting Party.

This limitation of liability also applies in the event of liability attributable to Namirial's Sub-suppliers.

The Client acknowledges that nothing will be due to it by Namirial as compensation, reimbursement, and/or indemnity, unless the Client provides documented evidence that the loss subject to compensation, reimbursement, or indemnity was caused by wilful misconduct or gross negligence of Namirial or of its employees, collaborators, or appointees.

The Client accepts that data stored on Namirial's infrastructure and/or on a shared system may be quarantined or deleted if such data is infected by a virus or otherwise corrupted, and has, in Namirial's sole discretion, the potential to infect or damage the system or data of other Clients hosted on the same infrastructure.

Where present and where circumstances permit, the clauses contained in this article also apply in favour of the Partner.

12. Force Majeure

No delay, failure, or non-performance will constitute a breach of this Contract to the extent it is caused by hurricanes, earthquakes, epidemics, or other natural causes, strikes or other labour disputes, riots or other acts of civil disorder, acts of war, terrorism, acts and orders of competent authorities such as expropriations, condemnations, embargoes, or other causes beyond the reasonable control of the Parties. Each Party undertakes to promptly notify the other of any force majeure events preventing the regular performance of the Contract. Should the force majeure situation persist for a period exceeding 60 (sixty) days, each Party may withdraw from the Contract, in whole or in part, by giving reasonable notice.

13. Contract Amendments

The Client agrees that Namirial, if present also through the Partner, may unilaterally amend the Contract, including the methods of providing the Services and Software, where the amendments become necessary:

i. under applicable law, including, by way of example, a change in such law;
ii. following an order issued by a public authority under applicable law;
iii. following the evolution of the Services and Software subject to the Contract;
iv. for technical reasons;
v. to make improvements to the Contract and/or the Services and Software that benefit the Client;
vi. to update the User interface and the User flow within the Services and Software without this having any negative impact on the functionalities of the Services and Software themselves;
vii. in the event of a subsequent excessive onerousness of the agreed performance.

Namirial, if present also through the Partner, shall inform the Client of the amendment before it takes effect, in accordance with the methods indicated in Article 16.
Namirial undertakes to ensure the improvement of the Services and Software subject to the Contract and, to this end, the Client acknowledges that Namirial may, at any time, modify the technical characteristics of the Service, eliminate functionalities, or discontinue access to applications or other IT resources.
Without prejudice to the right to the annual revaluation of the Economic Conditions under Article 6, the Client also acknowledges Namirial's right to make amendments that result in a worsening or increase of economic or performance terms, upon prior written notice received by the Client at least 30 (thirty) days before the amendments take effect. In such case, the Client is entitled to withdraw from the Contract with reference only to the Services and/or Software affected by the amendment, by sending written notice within 30 (thirty) days of receipt of the notice from Namirial, if present also through the Partner, in accordance with the methods established in Article 16. In the absence of withdrawal within the time and manner indicated, the amendments will become definitively effective and binding and will be deemed known and accepted for all purposes.
During the period in which the Services and Software are provided, the Client may always request Namirial, if present also through the Partner, to activate new Services and Software, new functionalities, or extend the assigned resources, which the Parties undertake to formalize in writing by signing the new Commercial Proposal and, where applicable, an amendment to the Data Processing Agreement and any Additional Conditions. The requested changes will be effective, constituting for all purposes an integration of the Contract, from the moment the related Commercial Proposal is signed. In any case, these General Conditions, in their most up-to-date version published on the Namirial Group's website, automatically apply from the moment the further requested Services and Software are activated and made accessible to the Client.
Contract amendments may concern all or only part of the Services and Software subject to the Contract.

14. Duration and Withdrawal

The duration of the Contract shall be that indicated at the time of purchase and reported in the membership form or in the Commercial Proposal.
Specifically:
- Software under a perpetual licence has no expiry date;
- Software under a subscription licence, including the related Connected Services, shall have a duration of one year from activation; upon expiry, the Contract shall be tacitly renewed on a year-by-year basis, unless notice of termination is sent to the domicile of the other party at least 90 (ninety) days before expiry by registered letter with acknowledgement of receipt or by certified email (PEC);
- the Connected Services, which may be activated as additional services in the case of the purchase of Software under a perpetual licence, shall have a duration of one year from activation; upon expiry, the Connected Services shall be tacitly renewed on a year-by-year basis, unless notice of termination is sent to the domicile of the other party at least 90 (ninety) days before expiry by registered letter with acknowledgement of receipt or by certified email (PEC).

Should automatic renewal be prohibited under applicable law, the Contract shall terminate upon expiry of the initial term.
Namirial or, if present, the Partner, reserves the right to withdraw from the Contract at any time, by giving notice to the Client in accordance with the methods indicated in Article 16, with at least 180 (one hundred eighty) days' notice.
Under Article 1373 of the Civil Code, each Party may withdraw from this Contract without having to pay the other Party any amount as compensation, reimbursement, or indemnity of any kind, if:

i. the other Party becomes subject to any insolvency procedure;
ii. the voluntary or judicial liquidation of the other Party occurs, or an administrative or judicial measure or decision is issued which, due to a matter attributable to it, orders the temporary and/or partial closure of the other Party;
iii. or in any case in which the other Party ceases, even partially, its business activity.

Upon expiry of the above-mentioned term, the Contract shall be deemed terminated.
Without prejudice to the Client's obligation to settle any fees due for the Services provided and the Software supplied and not yet paid, in the event of withdrawal, Namirial or, where applicable, the Partner shall refund to the Client any amounts received in advance as consideration, less the portion corresponding to the Services and Software already provided.
Withdrawal may concern all or only part of the Services and Software subject to the Contract.
The Client acknowledges and accepts that the Services and Software under this Contract are not subject to any trial period.
In the case of purchase through Namirial's e-commerce platform, the Client is permitted to withdraw from the Contract within 14 (fourteen) days from the date it was entered into, provided that the Software has not yet been installed on any computer. In such case, the Client shall obtain a refund of the fee paid.
In the event of non-renewal of the Contract, if the Client has not activated Software under a perpetual licence, the Client shall, within 6 (six) months following the expiry date, destroy any copies made of the Software, giving simultaneous written notice thereof to Namirial.
In any case, all Software is equipped with IT controls that allow it to function properly for only one calendar year; the activation codes for each subsequent year are provided to the Client only if the Client has renewed the effects of this Contract

15. Termination of the Contract and Express Termination Clause

A material breach, even if partial provided it is significant, of the obligations undertaken by a Party upon signing this Contract shall entitle the other Party, after having served a written notice to perform within 60 (sixty) days of receipt thereof, to terminate this Contract, without prejudice to the right to compensation for any damages suffered.
In the event of repeated and continued violation by the Client of the obligations provided in Article 8, the usage rules provided in Article 9, the provisions of Articles 17 and 18, and/or the policies and procedures indicated in Article 21, Namirial or, if present, the Partner has the right to immediately terminate the Contract, without prejudice to the Client's liability for any damages caused.
In the event of repeated and continued failure to pay within the agreed terms, even with reference to only one of the Services and Software subject to the Contract, Namirial or, if present, the Partner has the right to terminate the Contract with reference to the single Service and/or Software or to all of them.
As from the effective date of termination of the Contract, the Service shall be deactivated with immediate effect, unless otherwise provided in the Additional Conditions, without the need for any prior notice. The amounts paid by the Client shall remain definitively acquired by Namirial as a penalty, without prejudice to Namirial's right to charge the Client for any further expenses or costs incurred as a result of the termination, should the amount of the penalty not be sufficient to compensate for the damage. In any case, Namirial retains the right to claim compensation for any further damages suffered.
Without prejudice to the Client's obligation to settle any fees due for the Services provided and the Software supplied and not yet paid, in the event of early termination of the Contract by the Client, Namirial or, where applicable, the Partner shall refund to the Client any amounts received in advance as consideration, less the portion corresponding to the Services and Software already provided.
Termination may concern all or only part of the Services and Software subject to the Contract.

16. Communications

Namirial undertakes to make the requests and communications provided for under this Contract in writing, sending them to the Client's digital domicile and/or telematic communication channel indicated in the Commercial Proposal, or to the one subsequently used by the Client for operational communications during the term of the Contract.
All electronic correspondence sent by the Client to Namirial shall be sent to the following certified email address (PEC): amm.namirial@sicurezzapostale.it, or to any other PEC address notified to the Client at least 30 (thirty) days in advance, or to the different PEC address indicated in the Additional Conditions and/or Specific Conditions of the Service or Software.
Communications and requests relating to the Connected Services are made through the dedicated channels set up by Namirial and made available on Namirial's website or in the Additional Conditions, or, where applicable, through any channels made available by the Partner.
Communications relating to the unilateral amendment of the Contract that do not require notice under this Contract may also be made by publishing the new documents in force on Namirial's website.

17. Confidentiality

All information communicated by one Party to the other, or of which the Parties may become aware during the performance of the activities carried out under this Contract, is strictly confidential and must be used solely for the correct execution of the Service ("Confidential Information").
Each Party undertakes to adopt all physical, logical, and organizational measures necessary to prevent the disclosure of, and protect the secrecy of, the other Party's Confidential Information from unauthorized access, in any case ensuring the same protection provided for its own Confidential Information.
The Parties undertake:

i. not to disclose the other Party's Confidential Information in any way, in whole or in part, to third parties, except for their respective collaborators to whom disclosure is necessary solely for the execution of the Contract;
ii. to inform its collaborators of the nature of the Confidential Information and to instruct them to treat it confidentially. Each Party undertakes, under Article 1381 of the Civil Code, to ensure that its collaborators comply with the confidentiality obligations and acknowledge their liability for any damages caused by them as a result of the violation of the obligations provided under this article;
iii. not to reveal to third parties the fact that the Confidential Information was provided by the other Party;
iv. not to use, process, or transmit the Confidential Information to generative artificial intelligence (AI) tools or other AI-based tools, software, or services that do not explicitly guarantee a level of protection and confidentiality equivalent to or higher than that required by applicable law (in particular, by EU Regulation 2016/679 - GDPR) and that do not unequivocally exclude the use of data for the training of their models, unless expressly agreed in writing by the other Party;
v. to verify in advance that any AI tool used complies with data protection, confidentiality, and intellectual property regulations, and undertakes to indemnify and hold harmless the other Party from any damage, liability, or expense arising from any improper or unauthorized use of corporate data.

It is understood that the Confidential Information may be disclosed:

a. to Authorities, including supervisory and control authorities, in the cases and within the limits in which disclosure is required by legislative or regulatory provisions;
b. exceptionally to third parties, only with the prior written consent of the other Party;
c. when required by mandatory statutory provisions and provided that it is done within the limits imposed by such provisions.

The confidentiality obligation does not apply to Information that:

A. is already in the public domain before the signing of the Contract;
B. is or becomes available to the public for reasons other than disclosure by a Party, or by one or more collaborators, or otherwise for reasons that do not constitute a breach of the obligations established by this Contract;
C. is made available to a Party, on a non-confidential basis, by a source that, to the best of its knowledge, is not bound by a confidentiality agreement.

The confidentiality obligations under this article shall remain in force for 2 (two) years after the termination, for any reason, of this Contract, without prejudice in any case to the provisions of Articles 98 and 99 of Legislative Decree No. 30 of 10 February 2005, as subsequently amended ("Industrial Property Code").
Each Party undertakes to bind any third parties, sub-suppliers, and external collaborators of any kind who access the Confidential Information to the same obligations and guarantees provided under this article.

18. Intellectual Property

Namirial guarantees that the Services and Software provided to the Client under the Contract do not infringe any third-party rights. In particular, Namirial guarantees that it is entitled to make available the Software subject to the Contract as the owner of the intellectual and industrial property rights subsisting therein, or by virtue of specific licence agreements signed with the relevant third-party owners. The Client remains in any case fully responsible for the use of the Services and the use of the Software in accordance with the provisions of this Contract and applicable law.
The Parties acknowledge that the intellectual or industrial property rights vested, by way of example only and not limited to, in information, documents, files, elements, procedures, communications, technologies, assets, methodologies, and know-how ("IP Rights") remain the property of the Party or of the third-party owner or licensor. In no case does this Contract entail an assignment of such rights.
Any product or service that may be developed by Namirial during the performance of the Contract remains the property of Namirial.
The Client undertakes not to remove or modify trademarks or copyright notices referring to the IP Rights of Namirial or of third parties. The Client undertakes not to make available to third parties the programs or the results of the provision of services for commercial purposes.
Should a third party assert a claim that the Services or Software infringe an intellectual or industrial property right, Namirial may, at its own discretion and expense, (i) replace or modify, in whole or in part, the Service or Software subject to the infringement, or (ii) procure for the Client a licence enabling it to continue using the Service or Software, provided that the Client: (a) has fulfilled all of its obligations under the Contract; (b) notifies Namirial in writing, within seven (7) calendar days, of the infringement claim or the statement preceding it; and (c) cooperates in good faith with Namirial, providing all elements, information, and assistance necessary for the defence. Where none of the above measures is reasonably feasible, Namirial may terminate the Contract, in whole or in part, and refund the Client the fees paid for the affected Service or Software, less the portion corresponding to the period of use already elapsed.
The provisions of this article set out the entire liability of Namirial in relation to the infringement of intellectual and industrial property rights arising from the use of the Services and Software.

19. Personal Data Processing

Each Party acknowledges and agrees that, for the purposes of entering into and performing this Contract, personal data of contact persons, employees, and collaborators of the other Party may be mutually processed. For such processing, each Party acts as an independent data controller and provides appropriate notice under Articles 13 and 14 of EU Regulation 2016/679 ("GDPR"). Namirial's privacy notice is available at the following address .https://www.namirial.com/it/documentazione/
Should the performance of this Contract involve the processing of personal data on behalf of the Client, the Client undertakes to appoint Namirial or, if present, the Partner, as data processor through a specific Data Processing Agreement, which identifies the specific processing activities entrusted for each Service and/or Software provided. The Client acknowledges and accepts that, where the provision of the Services and Software takes place through a Partner, Namirial will act as an additional data processor appointed by the Partner.
Should the performance of this Contract involve the processing of personal data on behalf of the Client, the Client, as Data Controller, instructs and authorizes Namirial, as Data Processor, to carry out, directly or through its Sub-processors, processing activities strictly necessary for the improvement of the contractual Services provided to the Client (including but not limited to: testing, optimization, calibration, and validation of models/algorithms, performance and resilience measurements, anomaly correction, security, and fraud prevention), in compliance with the Data Processing Agreement. It is expressly prohibited to use the data for independent purposes such as marketing, profiling, or the development of products/services unrelated to the Client's contractual Services.
Namirial may engage Sub-processors for the aforementioned activities, in compliance with the authorization procedures and the Client's right to object as provided in the Data Processing Agreement.

20. Non-transferability

The Contract is not transferable or assignable to third parties, unless expressly authorized by Namirial.

21. Compliance Clause

By signing this Contract, the Client declares that it is aware that Namirial has adopted the following policies and procedures.

A. Professional and business ethics (published on the website):https://www.namirial.com/it/esg/etica-aziendale/
   - Organizational Model of Management and Control for the prevention of crimes provided for under Legislative Decree 231/2001 committed in the interest or to the advantage of the Company;
   - Code of Ethics, whose main objective is the clear definition of fundamental ethical values, and which contains the general principles that must inspire the conduct of the Company's corporate bodies and their members, employees, collaborators, and consultants, in order to promote, through self-discipline and corporate governance techniques, the creation and maximization of value for shareholders, for those who work in the Company, and for the clientele the Company serves; it establishes, as an inescapable principle of the Company's work, compliance with current laws and regulations, and sets out the principles of conduct to be followed by all recipients in the daily performance of their activities and work duties;
   - Anti-corruption Policy, which outlines the general principles and rules of conduct to be followed in carrying out activities, the prohibited conduct, and the safeguard measures identified by the Company to mitigate the risk of corruption; it applies to Namirial, its subsidiaries/affiliates, and all Namirial partners, within the limits of compatibility, and is also shared with other affiliated companies in order to promote principles and conduct consistent with those expressed by the Company;
   - Whistleblowing Policy, with the aim of strengthening control over the effective application of, and compliance with, the Code of Ethics, the provisions and principles of internal policies and procedures, laws and regulations, as well as ensuring the integrity of the Company and effectively addressing potential critical issues at an early stage, reducing the risk of significant damage to the Company's business and reputation; the Whistleblowing Policy governs the process of submitting, receiving, analysing, and processing reports from anyone, including confidentially or anonymously, and applies to directors, managers, employees, and anyone who is, has been, or is about to enter into a working relationship/relationship of interest with the Company, as further specified in the Whistleblowing Policy;
   - Cybersecurity Statement, to provide customers, suppliers, and partners with detailed information on the security practices adopted in subsidiaries and affiliated companies and on how the information and data processed are managed, in compliance with all current regulations and the highest industry standards.

B. Social commitment policies (published on the website):https://www.namirial.com/it/esg/impegno-sociale/

- Diversity, Equity & Inclusion Policy, through which the commitment is affirmed to implement fair employment policies in all workplaces, to ensure that employees at all levels are treated with respect and consideration, and to safeguard the Company's compliance with laws and industry standards.
- Employment and Labour Standards Policy, which outlines the general principles that Namirial pursues in carrying out its activities, the virtuous conduct, and the protective measures identified to embrace the values of diversity, equity, and inclusion.

C. Environmental and safety policy (published on the website):https://www.namirial.com/it/esg/sostenibilita/
- Environment, Health and Safety Policy, which defines Namirial's commitments regarding environmental protection, resource efficiency, and the health and safety of employees, contractors, customers, and neighbouring communities. The Policy addresses the Company's approach to operating in compliance with applicable local and national regulations on environment, health, and safety (EHS).

D. International Trade Procedure:
- Definitions
  - "Sanctioned Person" means any person, whether or not having legal personality: a) included in any list of designated persons pursuant to Sanctions; b) located or incorporated under the laws of any country or territory subject to global Sanctions; c) directly or indirectly owned or controlled, as defined under the relevant Sanctions, by a person referred to in points (a) or (b) above; or d) who otherwise is, or will become during the performance of this Contract, subject to Sanctions.
  - "Sanctions" means any economic or financial sanction, trade embargo, or similar measures issued, administered, or enforced by any of the following (or by any agency of any of the following): a) the United Nations; b) the United States of America; c) the United Kingdom; or d) the European Union or any current or future member state thereof.
- Client's Representations and Warranties:
  a. The Client represents that neither it, nor any of its affiliates/subsidiaries or holding companies, nor any of its directors, officers, and employees, is a Sanctioned Person.
  b. The Client shall, as soon as it becomes aware, promptly provide Namirial with details of any claim, action, lawsuit, proceeding, or investigation against it in relation to the Sanctions.
  c. The Client understands that Namirial must not receive any payment or transaction from a Sanctioned Person or in a manner that could result in a violation of the Sanctions. Namirial may therefore immediately suspend the provision of the Software and Services to the Client, should the Client violate any Sanction, representation, or undertaking of this Section.

The Client undertakes to act in compliance with the above-mentioned policies; it represents that it has no ongoing legal proceedings nor any convictions and/or measures of any kind for the offences contemplated by the policies and laws referred to above.
The Client undertakes to comply with requests for information or the production of documents from Namirial.
Any new policies adopted by Namirial and published on the aforementioned websites shall apply and be subject to the same conditions as those set out herein, upon email notification sent by Namirial.

22. Applicable Law and Jurisdiction

The Contract is governed by Italian law.
For any dispute that may arise between the parties in connection with this Contract and its subsequent amendments and integrations, the court of Ancona shall have exclusive jurisdiction.

23. Final Provisions

Any amendment and/or integration to this Contract, excluding the cases of unilateral amendment governed by Article 13 above, shall be valid and effective only if negotiated and formalized in writing by the Parties.
The possible nullity of all or some of the clauses of this Contract shall not extend its effects to the other contractual provisions. In such event, the Parties shall replace, in good faith and if and to the extent possible, the null clauses with other provisions having equivalent or similar content.
The Client authorizes Namirial and the Namirial Group companies to mention its corporate name and/or trademark on their websites and, more generally, on all their advertising material, exclusively for the purpose of disclosing to third parties the list of Namirial's client names.
The Parties waive the right to raise objections without having first fulfilled their own obligations. Any tolerance by one Party of the non-performance or violation of the Contract by the other Party shall not constitute, nor be interpreted as, a waiver of the rights due to each Party as a result of such non-performance or violation.
This Contract cancels and replaces any previous agreements concerning the Services and Software.

Client Signature* _____
* Please provide a digital signature

Client Name _____

ONEROUS CLAUSES
Pursuant to and for the purposes of Articles 1341 and 1342 of the Civil Code, the Client declares to have understood and expressly accepts the clauses contained in the General Terms and Conditions of Contract, under the following articles: Art. 4 (Object); Art. 6 (Economic Conditions, Invoicing and Adjustment of Fees); Art. 7 (Namirial's Obligations and Guarantees); Art. 8 (Client's Obligations); Art. 9 (Rules of Use of the Services and Software); Art. 10 (Suspension); Art. 11 (Liability); Art. 13 (Contract Amendments); Art. 14 (Duration and Withdrawal); Art. 15 (Termination of the Contract and Express Termination Clause); Art. 17 (Confidentiality); Art. 18 (Intellectual Property); Art. 20 (Non-transferability); Art. 21 (Compliance Clause); Art. 22 (Applicable Law and Jurisdiction); Art. 23 (Final Provisions).

Client Signature* _____
* Please provide a digital signature

ADDITIONAL CONDITIONS FOR THE SUPPLY OF SOFTWARE IN SAAS MODE

Section I - General Provisions

1. Value of these Additional Conditions

These Additional Contract Terms (hereinafter "Additional Conditions") govern the supply of Namirial Software provided in Software as a Service ("SaaS") mode. These Additional Conditions supplement the General Terms and refer to the services indicated in the Commercial Proposal. In the event of a conflict between the General Terms and the Additional Conditions, the latter shall prevail. The Definitions indicated in the General Terms apply to these Additional Conditions.

2. Service Object

The supply allows the Client to use the SaaS for the purposes indicated in the Contract, under the terms and conditions specified in these Additional Conditions, any specific Conditions, and as indicated in the technical documentation published on the website https://www.namirial.com/en/ (hereinafter "Technical Documentation"). The supply of SaaS includes, for the entire duration of the Contract, the Connected Services according to the methods and terms defined in article 5 of these Additional Conditions, as well as any additional connected and/or accessory services indicated in the Contract.
Unless otherwise expressly agreed, the following services are not included in the supply:

a. interventions for the restoration of archives and services caused by non-compliant use of the SaaS or otherwise due to culpable acts attributable to the Client (e.g., negligence, failure to comply with Usage Rules, tampering by personnel, etc.);
b. intervention and/or maintenance activities on the Client's infrastructure (e.g., firewall, networking devices, switches, Wi-Fi, client workstation configuration, printers, and/or other local network peripherals).

3. Content

The content consists of all data or information that the Client provides, authorizes for access, or inputs into the Software. Namirial will not have the ability to access, view, or listen to any Client content unless reasonably necessary to execute the Software. The Client represents and warrants that they own all rights to the content they submit; that such content is truthful and accurate; and that the use of the content provided by the Client does not violate these Additional Conditions, any specific Conditions, the General Terms, or applicable law. The Client acknowledges and agrees that they are solely responsible for the content provided and that they have full responsibility for the legal validity and copyright of the content.

4. Data Portability

With SaaS, unless otherwise provided in the Contract, a connected document archiving service is not provided, nor does the Software constitute an archiving tool. Notwithstanding the above, and unless otherwise specifically agreed, Namirial guarantees the Client the availability and the ability to extract (via download) the data and documents processed by the Client through the Software for the entire duration of the Contract, as well as for the additional period following the termination of the Contract specified in the Technical Documentation. After this period, Namirial will proceed with the deletion of data and documents and any other Client content. The Client has the option to activate a paid archiving and/or substitute storage service for the period following the termination of the Contract, which will be governed by specific contract terms.

5. Connected Services

The Connected Services include:

a) corrective maintenance service, which includes the diagnosis and removal of the causes and effects of Software malfunctions;
b) adaptive maintenance service, which includes the release to the Client of Software updates following any legislative, regulatory, or administrative changes ("regulatory requirements"), which entail variations attributable to the concept of ordinary administration and which do not involve the creation of a new Software module or a different product. Adaptive maintenance does not include the implementation or removal of new functionalities, even if the intervention is necessary to meet a regulatory requirement, except for functionalities implemented at Namirial's initiative. In any case, adaptive maintenance interventions are considered included in the economic conditions agreed in the Contract if the total working effort for all interventions in the reference calendar year (effort) is equal to or less than 20 (twenty) working days;
c) the release to the Client of any new versions of the Software that Namirial, or its licensors, may make available; therefore, the sending of additional Software modules and/or newly designed Software is excluded;
d) the release to the Client of any corrections of errors or malfunctions present in the Software, as soon as they are available;
e) SaaS software assistance is provided during the normal working hours observed by Namirial personnel or, if present, by the Partner. The service does not include the provision of assistance at the Client's premises. Assistance may be provided by Namirial, even remotely, through remote access to the Client's computer, previously and each time authorized by the latter, with the direct acceptance of each intervention request. Assistance requests are guaranteed through the channels indicated on the website https://www.namirial.com/en/.

The Service will be provided to the Client limited to the last two supported versions of the Software, without considering any modifications or integrations made by the Client or third parties appointed by the latter on the Software itself. Namirial, for the provision of assistance, may also

use third parties outside its organization or directly from authorized resellers. If Namirial needs to proceed with the maintenance of the Software and/or infrastructures, where this involves an interruption of the Software functionalities, it will inform the Client at least 24 (twenty-four) hours in advance about the need to carry out these interventions, as well as their duration, through publication on the website https://status.namirial.com/. The Client acknowledges and accepts that, in all phases of assistance, Namirial or Partner operators, even external to the organization, may become aware of the Client's personal data found during the connection phases on the latter's IT devices.

6. Warranties

Namirial guarantees the conformity of the Software to the specifications contained in the Technical Documentation, without prejudice to the fact that Namirial does not guarantee that these specifications meet the Client's needs or that the quality of the Software will meet the Client's expectations. The warranty provided by Namirial is conditioned on the proper functioning and adequacy of the IT equipment and connectivity services available to the Client, as well as the proper use of the Software by the latter.

7. Intellectual Property

All intellectual and industrial property rights, including the related economic exploitation rights on the SaaS, documentation, updates and developments, preparatory works, and derivative works are and remain, in whole or in part and worldwide, the exclusive property of Namirial. The Client undertakes, also pursuant to art. 1381 c.c., for each User, to use the SaaS in compliance with Namirial's intellectual property rights. Therefore, by way of example and not exhaustive and in any case without prejudice to the mandatory legal limits, the Client may not:

a) circumvent the technical limitations and technological protection measures present in the Software, including the authentication system;
b) reproduce, modify, adapt, customize the Software or create derivative works from it.

Namirial retains all rights to user manuals, videos, presentations, or any accessory printed material, including trademarks, logos, names, domain names, and other distinctive signs associated with the SaaS, with the consequence that the Client may not use them in any way without Namirial's prior written authorization.

8. Security

The authentication credentials provided by Namirial are considered known exclusively by the Client, who is required to keep them confidential and with the utmost diligence, undertaking not to transfer them and not to allow third parties to use the Software in any way; otherwise, the Client will be considered responsible for any damage or prejudice caused directly or indirectly to Namirial and/or third parties due to the improper use of the Software by unauthorized persons. The security of the workstations and resources used for the services provided by Namirial is the responsibility of the Client. The Client therefore undertakes to ensure that account management is monitored according to current security procedures to limit the hypotheses of access attempts and/or violations through their systems. The Client also undertakes to ensure that log procedures are secure and verified and that access management is preordained to traceability and monitoring procedures. Namirial uses physical, electronic, and managerial procedures to safeguard and prevent unauthorized access to the Client's Content. Namirial chooses these guarantees based on the sensitivity of the information collected, processed, and stored and the current state of technology. Although Namirial takes measures to safeguard the disclosure of unauthorized information, the Internet and Software are not 100% secure, so Namirial will not guarantee the Client that the information collected or stored will be protected from all unauthorized access. Further specific security provisions are contained in Sections I and II of these Additional Conditions, applicable, respectively, in the case of service use through "Shared SaaS" or "Private SaaS".

9. Personal Data Processing

In the context of the supply of Namirial Software under these Additional Conditions, the Client, as Data Controller, undertakes to appoint Namirial as Data Processor pursuant to art. 28 of the GDPR through a Data Processing Agreement that will regulate in detail, also through specific processing sheets, depending on the type of Namirial Software used by the Client, the terms, methods, and responsibilities of the processing. However, if the Namirial Software provided to the Client is connected to the provision of Qualified Services by Namirial, the latter will act as Data Controller of the personal data. If the Client, for their exclusive purposes, needs to access the personal data of Users collected by Namirial in the context of the provision of Qualified Services, they will act as an independent Data Controller.

Section II - Shared SaaS security

10. Shared SaaS Security

These security clauses apply to the provision of software in "Shared SaaS" mode. Shared SaaS means a software distribution model in which multiple Clients share the same infrastructure, platform, and applications, hosted and managed by Namirial, as the Service provider.

11. Software and Server Operating System Update Periods

Patches and updates to new versions are managed by Namirial in accordance with its security policies and schedule. They cannot be delayed at the Client's request. The Client who needs a customized patch and update program must switch to private SaaS software.

12. Web Application Firewall

The Web Application Firewall (WAF) is enabled by default to ensure the protection of "Shared SaaS" software. The WAF cannot be disabled at the Client's request. The Client who needs full control over the WAF configuration must request the activation of the "Private SaaS" delivery mode.

13. Penetration Testing and Vulnerability Assessment

The Client cannot perform penetration testing or vulnerability assessments on Namirial's public shared multi-tenant infrastructure.

14. Audit and Test Execution

The Client is not authorized to participate in the execution of security tests. Namirial has implemented advanced Business Continuity (CO) and Disaster Recovery (DR) policies that include testing activities. Tests are carried out according to Namirial's schedule and in accordance with internal policies.

Section III - Private Saas Security

15. Private SaaS Security

These security clauses apply to the provision of software in "Private SaaS" mode. "Private SaaS" means a software distribution model in which the application and infrastructure are dedicated exclusively to a single Client, while maintaining the typical advantages of the SaaS model, such as centralized management, maintenance, and updates managed by the provider.

16. Updates

Patches and updates to new versions can be managed individually by mutual agreement. Namirial informs the Client when patches or updates are available. The Client must refuse the patches within 9 (nine) days, after which they will be considered approved. If the Client refuses the patches, Namirial cannot be held responsible for incidents related to the obsolescence of the Operating System and software. To receive maintenance, the Client must use a Long Term Stability (LTS) version no older than 2 years or the current released version, which is also distributed in "Shared SaaS" Software.

17. Web Application Firewall

The Web Application Firewall (WAF) is not enabled by default in "Private SaaS" software. A support service is available on request to activate the WAF.

18. Penetration Testing and Vulnerability Assessment

Penetration testing and vulnerability assessments can only be performed if the "Private SaaS" software is accessible via a custom domain. A support service is available on request for the execution of penetration testing and vulnerability assessments.

19. Custom Domain Name

The Client must provide custom domain names (e.g., sign.Clientname.com or similar) for "Private SaaS" software; failure to do so will result in no access to the service. In any case, Namirial has the right to register a custom domain on behalf of the Client, on which the service will be provided directly or via URL redirection.

20. Audit and Test Execution

The Client is not authorized to participate in the execution of tests. Namirial has implemented advanced Business Continuity (CO) and Disaster Recovery (DR) policies that include testing activities. Tests are carried out according to Namirial's schedule and in accordance with internal policies.

Section IV - Specific Service Conditions

These Additional Conditions are accompanied by specific Conditions for the provision and use of certain SaaS Services that require specific regulations. They constitute an integral and essential part of the Contract.

Client Signature* _____
* please provide a digital signature

Client Name _____

GENERAL DATA PROCESSING AGREEMENT

Article 28 Reg. EU 2018/679 ('**GDPR**')

Between

The Client, as identified in the Contract ("Controller"), represented by its legal representative with the necessary powers, in the capacity of,

Data Controller

and

Namirial S.p.A., with registered office in Senigallia (AN), Via Caduti sul Lavoro, 4, 60019 – Tax Code N. 02046570426**,** phone 071/63494, e-mail/PEC amm.namirial@sicurezzapostale.it ('**Processor'** or '**Supplier**'), represented by its legal representative with the necessary powers, in the capacity of

Data Processor

Furthermore, the Controller and Processor may be jointly referred to as '**Parties'** and individually as '**Party'**.

WHEREAS

I. The Parties have entered into one or more contracts ('**Contract'**) for the provision of Services ('**Services'**);
II. The Contract involves the processing of information defined by law as personal data, and the Parties, therefore, intend to regulate, within this General Data Processing Agreement ("**Agreement**"), the terms and conditions for the processing of personal data carried out by the Processor in the context of providing the Services under the Contract;
III. The details and specific characteristics or particular conditions of the personal data processing are contained within the so-called "**Processing Sheets**" related to one or more Services activated by the Client, which will be attached to this Agreement from time to time.
IV. These Processing Sheets will detail the operational methods of processing in relation to the specific Service, indicating, where applicable, the list of Sub-Processors and any additional security measures applied. The Processing Sheets, once signed, will be included as further Annexes to this Agreement and will form an integral and substantial part of it;
V. Before entrusting the Processor with the performance of the Services, the Controller has verified the Processor's experience, capacity, and reliability, and has assessed that the Processor offers sufficient guarantees to implement appropriate technical and organizational measures and to ensure adequate protection of the processed data and the rights of the data subjects;
VI. The Processor must carry out the Processing operations in accordance with the instructions provided in writing by the Controller through a contract or other binding legal act specifying the duration, nature, and purposes of the Processing, the categories of personal data processed, and the categories of data subjects involved in the Processing, as well as the Processor's obligations and rights regarding the Processing;
VII. With this Agreement, the Controller intends to appoint the Processor indicated in the preamble as the data processor and provide all necessary instructions for the Processing of personal data underlying the provision of the Services;
VIII. The Controller authorizes the Processor, as well as the persons authorized by the latter, to access only the personal data strictly necessary for the execution of the Contract (**Personal Data**');
IX. This Agreement does not entail any right of the Processor to specific fees and/or indemnities and/or reimbursements, other than those already possibly provided for in the Contract, except for further implementations specifically requested and agreed upon between the Parties in a separate written agreement;
X. In the event that the Client acts as a Data Processor on behalf of another controller (the "Final Client"), the Client itself will assume, in relation to such specific processing, the obligations and responsibilities of a

data processor towards Namirial, which in this context will assume the role of Sub-Processor. In such a situation, the provisions relating to data processing and the Processor's obligations under this Agreement will apply, but with the Client acting as Processor on behalf of the Final Client and Namirial acting as Sub-Processor on behalf of the Client;

XI. In any case where the Client acts as Controller or Processor on behalf of the Final Client, Namirial agrees to act as Processor and/or Sub-Processor and, therefore, undertakes to process the Personal Data in accordance with the instructions received from the Client and in a manner that ensures the protection of the Personal Data itself, according to the security measures established in this Agreement and the Processing Sheets attached to it

NOW, THEREFORE, THE PARTIES AGREE AND STIPULATE AS FOLLOWS

1. VALIDITY OF THE PREMISES AND ANNEXES. DEFINITIONS

1.1. The premises and Annexes constitute an integral and substantial part of this Agreement.

1.2. Unless otherwise provided in this Agreement, all capitalized terms used in this Agreement and the Annexes shall have the meaning attributed to them in the Contract and shall be understood to be expressed in both singular and plural forms. In accordance with the definitions contained in the applicable law, the terms and definitions set forth in **Annex I – Definitions** to this Agreement are used, to which reference is made.

1.3. The Processing Sheets related to the Services used by the Client may access this Agreement, even at a later time, in case of integration of the Contract for the activation of new Services. In such a case, the Annexes, signed by the Parties together with the contractual addendum, access this Agreement.

2. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

2.1. The Controller entrusts the Processor with all – and exclusively – the Processing operations of Personal Data necessary for the full execution of the Contract.

2.2. The Controller declares to comply with all obligations provided by the Applicable Law within its competence in relation to the Processing of Personal Data under this Agreement. In particular, the Controller:

a. has the right and obligation to make decisions regarding the purposes and means of the Processing, including identifying the correct legal basis for the Processing;
b. declares that the Personal Data is relevant and not excessive concerning the purposes for which it was collected and subsequently processed, and is transmitted in compliance with all requirements provided by the Applicable Law;
c. prepares and – where necessary – makes available to the Processor adequate and complete information on the Processing of Personal Data pursuant to art. 13 and/or art. 14 of the GDPR.

2.3. The Controller undertakes to officially notify the Processor of any changes that may be necessary concerning the Processing operations of Personal Data. The Processor and its Authorized Persons will not carry out Processing operations of Personal Data other than those indicated by the Controller under this article.

2.4. The Controller guarantees that the infrastructures and systems possibly made available by the Controller and/or by third parties appointed by the latter, on which the Processor will be called to carry out the Processing ('Controller's Systems'), are adequate and comply with the reference standards and sector regulations and are capable of ensuring the regular provision of the Services in compliance with this Agreement. The Controller therefore undertakes to indemnify and hold the Processor harmless from any disruption, damage, or interruption in the execution of the Processing that may result from the inadequacy, anomalies, and/or any malfunctions of the Controller's Systems on which the Processor is called to operate.

3. OBLIGATIONS OF THE PROCESSOR

3.1. Within the limits of its competence under the Contract and this Agreement, the Processor shall be required, for itself and its Authorized Persons, to comply with the provisions of the Applicable Law, with particular regard to the provisions of the GDPR, the Privacy Code, as well as the applicable measures of the competent Supervisory Authorities imposing specific obligations on data processors;

3.2. In particular, the Processor shall carry out the Processing operations assigned to it in accordance with the instructions given by the Controller contained in this Agreement, as well as those subsequently notified by the Controller in writing with reasonable notice.

3.3. The Processor shall carry out the Processing operations functional to the tasks assigned to it in accordance with this Agreement and the purposes for which the Personal Data is collected and processed. Where a

different and exceptional processing of Personal Data is necessary compared to that covered by this Agreement, the Processor undertakes to inform the Controller in advance and promptly, who may object.

3.4. The Processor is required to manage the documentation relating to the Processing entrusted to it through appropriate procedures, according to criteria of efficiency and ensuring the custody, non-alteration, and easy retrieval of any relevant document for compliance with the requirements imposed by the GDPR.

3.5. The Processor makes available to the Controller all the information and documents necessary to demonstrate compliance with the obligations provided for in art. 28 of the GDPR; allows and contributes to audit activities, including inspections notified with reasonable notice, carried out by the Controller or by a third party appointed by the Controller.

3.6. The Processor immediately informs the Controller if, in its opinion, an instruction violates the GDPR or other provisions of the Applicable Law. Furthermore, the Processor assists the Controller, at the latter's request, in proceedings before the competent Supervisory Authority or judicial authority, in relation to the Processing activities within its competence, in particular by making available any information and documents useful for demonstrating compliance with the obligations under the Applicable Law regarding the Processing of Personal Data.

3.7. The Processor promptly communicates to the Controller any requests from Data Subjects, objections, inspections, or requests from Supervisory and judicial Authorities, as well as any other relevant information in relation to the Processing of Personal Data.

3.8. The Processor identifies, within its organizational structure, the Authorized Persons to carry out Processing operations of Personal Data. Upon appointment, the Processor provides the Authorized Persons with adequate written instructions on the methods of Processing, in compliance with the provisions of art. 29 of the GDPR and this Agreement. By way of example and not exhaustively, the Processor, in designating the Authorized Persons in writing, prescribes that they have access only to Personal Data whose knowledge is strictly necessary for the performance of the tasks assigned to them (need-to-know principle). The Processor must also verify that the Authorized Persons apply all security measures relating to the custody of access credentials in case of Processing carried out through electronic means. The Processor also verifies that the Authorized Persons securely store non-IT media containing any copy of the Personal Data, particularly if belonging to Special Categories. Finally, the Processor ensures that the Authorized Persons are bound by effective confidentiality obligations, even for the period following the termination of the employment relationship with the Processor, in relation to the Processing operations of Personal Data carried out by them.

3.9. In the event of damages resulting from the Processing, the Processor shall indemnify and hold the Controller harmless from any damage if the Processor has not complied with the obligations of the GDPR specifically addressed to data processors, or has acted in a manner contrary to the legitimate instructions of the Controller, pursuant to arts. 83 et seq. of the GDPR.

3.10. Where applicable and in relation to the Processing carried out, for the execution of the Contract, by the Authorized Persons with the role of 'System Administrator', the Processor is also required to comply with the provisions contained in the Privacy Guarantor's Measure of 27 November 2008, as amended by the Measure of 25 June 2009. To this end, in particular, the Processor directly and specifically retains the identifying data of the Authorized Persons appointed as System Administrators and provides them to the Controller upon request.

3.11. Pursuant to Article 28(3)(a) of the GDPR, the Controller includes among the instructions to the Processor the execution of processing operations strictly necessary for the following activities aimed at improving the Services covered by the Contract: testing, performance measurement and optimization, calibration and validation of models/algorithms, improvement of accuracy/reliability/usability, security and fraud prevention, correction of bugs and anomalies, insofar as they are functional to the proper provision of the Services to the Controller. Any use for the autonomous purposes of the Processor or its Sub-processors, including marketing, profiling, or the development of unrelated products/services, is excluded.

3.12. The improvement activities referred to in the preceding paragraph shall be carried out only to the extent strictly necessary for the provision, maintenance, and security of the Services, or otherwise on anonymized/aggregated data, unless otherwise instructed and legally justified by the Controller. The Processor may engage Sub-processors, provided that it imposes a prohibition on data reuse and on the training of general-purpose models, as well as the obligation to delete the data upon completion of the activities.

4. SECURITY OF PROCESSING

4.1. Within the limits of its competence under the Contract and this Agreement, the Processor is required, for itself and its Authorized Persons, to implement the Security Measures provided by the Applicable Law, as well as those indicated by the Controller, assisting the latter in ensuring compliance with art. 32 of the GDPR.

4.2. In the context of the personal data processing activities related to the provision of the Services, the Supplier undertakes to adopt appropriate technical and organizational measures to prevent unlawful or unauthorized processing, as well as to protect Personal Data from destruction, alteration, loss, unauthorized access, or disclosure, as detailed **in Annex II – Technical and Organizational Security Measures** of this Agreement.

4.3. **Annex II** describes the measures adopted by the Supplier to ensure the confidentiality, integrity, availability, and resilience of systems and Services, as well as the procedures for the timely restoration of access to Personal Data in the event of a security incident. The implemented measures ("***Security Measures***") are defined in relation to the level of risk associated with the processed Personal Data, considering the state of the art, implementation costs, and the nature, context, and purposes of the processing. The Client acknowledges and agrees that these measures are adequate to ensure a level of security compliant with the applicable regulatory requirements.

4.4. The Supplier reserves the right to update or modify the Security Measures to ensure constant adaptation to technological and regulatory developments, provided that such changes do not reduce the overall level of protection of the Services.

4.5. If the Client requests the adoption of specific additional security measures beyond those provided, the Supplier will assess the technical and operational feasibility of such requests, reserving the possibility of applying additional costs for any implementations.

4.6. In the case of products installed at the Client's premises or those of third parties appointed by the Client (e.g., on-premises solutions), the Security Measures adopted by the Supplier will apply exclusively to the Services that involve the processing of Personal Data by the Supplier or its sub-processors (e.g., remote support and assistance activities or migration services).

4.7. In the event that the Services allow integration with third-party software or applications, the Supplier will not be responsible for the Security Measures applied by such parties or for any vulnerabilities resulting from the integration carried out directly by the Client or third-party suppliers.

4.8. Notwithstanding the security obligations of the Supplier, the Client is responsible for adopting all necessary measures to ensure the protection of Personal Data processed in the context of the use of the Services by its personnel or any authorized parties.

4.9. The Client undertakes to use the Services in compliance with security best practices and to ensure an adequate level of protection against the risks associated with the processing of Personal Data.

4.10. The Client must implement all appropriate measures to protect authentication credentials, devices, and systems used to access the Services, as well as to perform regular backups of Personal Data, in order to ensure their restoration in compliance with applicable regulations.

4.11. The Supplier will not be responsible for the protection of Personal Data that the Client or third parties process outside the Supplier's and its sub-processors' systems, including data stored on paper or on the Client's internal IT infrastructures (e.g., private data centers or on-premises servers).

5. SUB-PROCESSOR

5.1. Exclusively for the purpose of providing the Services covered by the Contract, and in accordance with the provisions of this Agreement, Personal Data may be processed by Sub-Processors identified by the Processor.

5.2. The Processor undertakes to select its Sub-Processors among persons whose experience, capacity, and reliability provide sufficient guarantees to implement adequate Security Measures, so that the Processing meets all the requirements of the Applicable Law and ensures the protection of the Data Subject's rights. As a result, the Processor undertakes to enter into specific contracts or other binding legal acts with the Sub-Processors, through which the Processor describes their tasks in detail and requires them to comply with the same obligations imposed by the Controller on the Processor under the Applicable Law and this Agreement.

5.3. In any case where a Sub-Processor fails to comply with its obligations regarding personal data protection, the Processor acknowledges that it retains full responsibility towards the Controller for the behavior of such Sub-Processor. As a result, the Processor undertakes to indemnify and hold the Controller harmless from any damage, claim, and request for compensation that may be made against the Controller as a result of the Sub-Processor's failure to comply with its obligations and, more generally, any violation of the Applicable Law by the Sub-Processor and any of its subcontractors and/or authorized persons.

5.4. The Processing Sheets identify and list the Sub-Processors appointed by the Processor and already approved by the Controller. The Processor also undertakes to inform the Controller in writing of any planned changes

or replacements regarding the Sub-Processors, giving the Controller the opportunity to object to such changes within 30 (thirty) days of receiving the relevant communication.

5.5. The communication referred to in the preceding paragraph may alternatively be fulfilled by publishing the updated list of Sub-Processors in the "Documentation" section on Namirial's website (www.namirial.com).

6. TRANSFER OF PERSONAL DATA

6.1. The Processor declares that it will not transfer Personal Data outside the EEA, unless it is previously and specifically authorized in writing by the Controller. In case of authorization, the Processor may transfer Personal Data only on the documented instruction of the Controller and, in particular, in full compliance with arts. 44, 45, 46, and 49 of the GDPR.

6.2. In the case of transfers to third countries or international organizations required by EU or Member State law to which the Processor is subject, and which have not been requested by the Controller with a specific instruction, the Processor is required to inform the Controller of such obligation before the transfer, unless the law itself prohibits such communication for important reasons of public interest.

6.3. In any case of transfer of Personal Data outside the EEA, to the extent that there is no Adequacy Decision by the European Commission for the destination country of the Personal Data, the Processor is required to sign, and have the recipients of the Personal Data sign, the Standard Contractual Clauses in their latest version adopted by the European Commission, ensuring that the same obligations contained therein are guaranteed towards any further recipients of the Personal Data in the case of so-called onward transfer. If and where necessary, the Processor must also stipulate the adoption of any additional Security Measures in accordance with Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of personal data protection and Recommendations 2/2020 on European essential guarantees for surveillance measures adopted by the European Data Protection Board ('EDPB').

7. ASSISTANCE TO THE CONTROLLER

7.1. Taking into account the nature of the Processing and the information available to it, the Processor is required to provide support to the Controller so that the latter can fulfill the obligations imposed by the Applicable Law on data controllers, such as, by way of example and not exhaustively, the obligations to:

a. notify a Personal Data Breach to the competent Supervisory Authority without undue delay and, where possible, no later than 72 hours after becoming aware of it, unless it is unlikely that the breach will result in a risk to the rights and freedoms of natural persons;
b. conduct a data protection impact assessment (DPIA') related to the Processing governed by this Agreement, if such Processing presents the characteristics set out in art. 35 of the GDPR;
c. consult the competent Supervisory Authority pursuant to art. 36 of the GDPR, if a DPIA indicates that the Processing governed by this Agreement would result in a high risk in the absence of measures taken to mitigate the risk;
d. respond to requests to exercise Data Subjects' Rights, pursuant to Chapter III of the GDPR. Where the Processor receives such requests directly, the Processor shall (i) promptly inform the Controller in writing, attaching a copy of the request; and (ii) taking into account the nature of the Processing, assist the Controller with appropriate technical and organizational measures within its competence to fulfill such requests.

7.2. The Processor shall also promptly inform the Controller, and in any case within 48 (forty-eight) hours of receipt, by communication to the Notification Email address, of any dispute, inspection, or request from the Supervisory Authority and judicial authorities, as well as any other relevant information relating to the Processing of Personal Data covered by this Agreement

8. PERSONAL DATA BREACHES

8.1. In the event that the Processor becomes aware of a Personal Data Breach involving or potentially involving, even indirectly, the systems and Processing operations used on behalf of the Controller, or the Personal Data covered by this Agreement, the Processor undertakes to inform the Controller through formal communication sent to the Notification Email address, without undue delay and no later than 48 (forty-eight) hours after becoming aware of the Personal Data Breach.

8.2. Following the detection of an anomaly or a suspected Personal Data Breach covered by this Agreement, the Processor is required to initiate a preliminary analysis to collect data relating to the anomaly and, in any case,

all necessary information for the classification and management of the breach, including details relating to the nature of the incident, the data involved, the measures taken, and the intervention times.

8.3. The Processor undertakes to ensure compliance with the aforementioned timelines and to indemnify and hold the Controller harmless from any damage, claim, and request for compensation that may be made against the Controller as a result of the Processor's failure to comply with its obligations and, more generally, any violation of the Applicable Law by the Processor and any of its subcontractors and/or authorized persons.

8.4. In the event of a Personal Data Breach, the Processor undertakes to provide, to the extent of its competence and responsibility under the Contract, the maximum cooperation to the Controller and the competent Supervisory Authorities, in order to fulfill any applicable legal obligations (e.g., notification obligation to the Supervisory Authority, possible communication to Data Subjects, application of appropriate measures to mitigate or prevent risks and damages). In this regard, the Controller undertakes to promptly provide the Processor with proof of any communication exchanged with the competent Supervisory Authorities in which the Processor is in any way involved or mentioned.

9. DURATION. DELETION AND RETURN OF PERSONAL DATA

9.1. The appointment as Data Processor under this Agreement will have the same duration as the Contract, unless revoked earlier, in which case the appointment will continue to be effective as necessary to complete the Processing operations required for the termination of the relationship between the Parties or to fulfill legal obligations imposed on them.

9.2. Upon termination of the Processing operations entrusted, as well as upon termination for any reason of the contractual relationship with the Processor, the latter, at the discretion of the Controller, will be required to (i) return to the Controller the Personal Data subject to Processing, or (ii) proceed with the complete destruction of the Personal Data and each copy thereof, except in cases where data retention is required by law or pursues other legitimate purposes (e.g., accounting, tax purposes, etc.). In both cases, the Processor must provide the Controller with a written statement certifying that no copy of the Personal Data subject to this Agreement is held by the Processor.

10. AUDIT AND INSPECTIONS

10.1. The Processor makes available to the Controller all the information necessary to demonstrate compliance with its obligations under this Agreement and the Applicable Law, and will allow and contribute to audit activities, including inspections carried out by the Controller and/or a third party appointed by the Controller. For this purpose, upon written notice of at least 10 (ten) working days, the Controller and/or the persons appointed by it will have the right to access the premises of the Processor where the Processing takes place or where data or documents related to this Agreement are available. In any case, the Controller undertakes, for itself and for any third parties it may appoint, to use the information collected during the verification operations only for such purposes, and to carry out any verification under this article without reasonably prejudicing the regular conduct of the Processor's business activities.

11. COMMUNICATIONS BETWEEN THE PARTIES

11.1. For the purposes of this Agreement, the Processor declares that it has appointed a Data Protection Officer (DPO) domiciled at the Processor's headquarters, who can be contacted at the following address: dpo@namirial.com or at the following phone number: 071/63494.

11.2. The Processor will contact the Controller, in all cases provided for within this Agreement, through communication sent to the Notification Email address provided by the Controller.

11.3. The Parties undertake to promptly notify each other of any changes to their contact addresses. In the absence of such timely notification, communications sent to the outdated address will be considered valid and effective.

ANNEX I

DEFINITIONS

- **a)** '**Agreement'** means this Data Processing Agreement, including the premises and Annexes;
- **b)** '**System Administrators'** means the Authorized Persons responsible for the management and maintenance of a processing system or its components, as identified by the GPDP Measure No. 300/2008, containing Measures and precautions prescribed to data controllers processing data with electronic tools regarding the assignment of system administrator functions, and subsequent amendments;
- **c)** '**Supervisory Authority'** means any independent supervisory authority under Chapter VI of the GDPR, competent to monitor and ensure the application of legal provisions on personal data protection, with reference to the Processing of Personal Data carried out in the execution of the Contract (including the Italian Data Protection Authority or 'GPDP');
- **d)** **'Special Categories of Personal Data'** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as identified in art. 9 of the GDPR;
- **e)** **'Standard Contractual Clauses'** means the clauses adopted by the European Commission in Decision 2021/914/EU of 4 June 2021 for the transfer of personal data from a data controller established in the European Union ('EU') / European Economic Area ('EEA') to a non-EU or non-EEA entity acting as a data processor;
- **f)** **'Contract'** means the contract signed between the Parties for the provision of the Services;
- **g)** **'Personal Data'** means any information relating to an identified or identifiable natural person (Data Subject') processed by the Processor, on behalf of the Controller, in relation to the execution of the Contract;
- **h)** **'Data Subject's Rights'** means the rights recognized to the Data Subject by the Applicable Law. Within the limits of the applicability of the GDPR, 'Data Subject's Rights' means, for example, the right to request from the data controller access to, rectification or erasure of Personal Data, the right to restrict the Processing of the Data Subject's data or the right to object to the Processing, as well as the right to data portability;
- **i)** **'Notification Email'** means the email address (or addresses) provided by the Client at the time of signing the Contract or provided through another official channel to the Processor, to which the Client intends to receive notifications from the Processor;
- **j)** **'Applicable Law'** means the legislation on personal data protection applicable to the Processing of Personal Data underlying the Contract, such as EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('GDPR'), Legislative Decree No. 196 of 30 June 2003 and subsequent amendments, containing the Personal Data Protection Code ('Privacy Code'), as well as any other specific applicable legislation, including the measures, guidelines, and indications of the competent Supervisory Authorities;
- **k)** **'Security Measures'** means the technical and organizational measures, as per art. 32 of the GDPR, suitable to ensure an adequate level of security of Personal Data, as well as all necessary measures to prevent or at least minimize any reasonably foreseeable risk of destruction, loss, alteration, unauthorized disclosure or access, accidental or unlawful, to the processed Personal Data;
- **l)** **'Authorized Persons'** means the natural persons within the organizational structure of the Processor specifically identified in writing and authorized to access and process Personal Data in the context of the execution of the Contract, and who act under the control and according to the instructions of the Processor;
- **m)** **'Processor'** generally means the natural or legal person, public authority, agency, or other body that processes personal data on behalf of a data controller;
- **n)** **'Services'** means the services provided under the Contract;
- **o)** **'Controller's Systems'** means the infrastructures and systems possibly made available by the Controller and/or third parties appointed by the latter, on which the Processor is called to carry out the Processing;
- **p)** **'Sub-Processor'** means an entity identified by the Processor that carries out, in whole or in part, the Processing of Personal Data entrusted to the Processor, in compliance with the obligations and instructions established by the Controller, and that has been expressly authorized by the latter;
- **q)** **'Controller'** generally means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data;
- **r)** **'Processing'** means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage,

adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

ANNEX II

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. ORGANIZATIONAL SECURITY MEASURES

TYPE OF MEASURE	DESCRIPTION
Internal Policies and Regulations	The Processor has adopted a set of internal policies, procedures, and regulations, binding on all personnel authorized to process personal data. These policies and guidelines define the rules for the secure use of IT resources and provide specific internal regulations for information management, with mandatory compliance by all users. The objective is to ensure compliance with the principles of confidentiality, integrity, and availability of personal data, minimizing the risks of unauthorized access or misuse of information within all group companies.
Access Authorization and Logical Controls	The Processor defines access profiles in compliance with the least privilege necessary to perform the assigned tasks. Authorization profiles are identified and configured prior to the start of processing, to limit access to only the personal data necessary to perform processing operations. For more sensitive operations, two-factor authentication (MFA) is adopted to strengthen access security. These profiles are subject to periodic checks to verify the continued existence of the conditions for maintaining the assigned profiles.
Access Monitoring	Access to systems processing personal data is logged and monitored, with periodic analysis of logs to identify any anomalies or suspicious activities.
Change Management	The Processor has adopted a specific procedure regulating the Change Management process in consideration of the introduction of any technological innovations or changes in its organizational structure.
Incident Management and Business Continuity	The Processor has implemented a specific Incident Management procedure to ensure the restoration of normal service operations as quickly as possible, maintaining the best service levels. Incidents are classified by severity and impact on personal data. Personnel are trained to handle security events and execute containment procedures. Periodic tests are conducted on the organization's responsiveness to incidents. A Business Continuity Plan is implemented to ensure service resilience even in emergencies.
Measures to Ensure Limited Data Retention	The Processor follows the principles of Data Protection by Design and by Default. Technical measures: no more personal data is collected than necessary for the respective purpose; use of default settings that respect data protection. Organizational measures: data protection policy according to the principles of "privacy by design / by default" included in the SCS-P14 Group Privacy and Personal Data Protection Policy; OWASP Secure Mobile Development security checks are performed (see SCS-P08 Group Secure Coding Policy); perimeter analysis of web applications.
Data Breach	The Processor has implemented a specific procedure for managing events and incidents with a potential impact on personal data, defining roles and responsibilities, the detection process (suspected or confirmed), the application of countermeasures, the response and

	containment of the incident/breach, as well as the methods for promptly communicating personal data breaches to the Controller. For the Processor's part, this procedure at least identifies: the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records involved; the likely consequences of the personal data breach; the measures taken or proposed to address the personal data breach and, where appropriate, to mitigate its possible adverse effects.
Training	To ensure an adequate level of awareness, the Processor provides periodic training on the correct processing of personal data and information security. Training is mandatory for all personnel accessing personal data. Tests and checks are conducted to assess the level of understanding of security policies. Simulated cyber-attack campaigns (e.g., phishing tests) are organized to educate personnel on common threats. Training is periodically updated to reflect regulatory and technological developments.
Sub-Processor Management	When the Processor uses Sub-Processors, strict controls are implemented to verify their compliance with the required security measures. Each Sub-Processor is required to comply with security standards equivalent to those of the Processor. Periodic audits and inspections are conducted to verify supplier compliance. The Processor maintains an updated register of Sub-Processors.
Data Backup and Recovery	To ensure data availability and fault resilience, the Processor implements a backup and disaster recovery system that includes: periodic backups with defined retention policies; backup protection through encryption and controlled access; periodic tests to ensure rapid data recovery when needed; data replication in secure data centers to prevent the loss of critical information.
Procedures to Regularly Test, Verify, and Evaluate the Effectiveness of Technical and Organizational Measures to Ensure Processing Security	Internal policies related to security measures are periodically reviewed and confirmed for adequacy and effectiveness during ongoing internal audits and annually by independent, external, and accredited certification bodies as part of ISO 9001 and ISO 27001 monitoring and recertification audits.
CISO Appointment	To ensure an adequate level of information security and compliance with applicable regulations, the Processor has appointed a Chief Information Security Officer (CISO) with the primary task of: overseeing the implementation and effectiveness of security measures adopted for the protection of Personal Data; monitoring the evolution of cyber threats and promoting the continuous updating of security policies; coordinating security incident response activities; defining security improvement strategies for the protection of corporate assets. The CISO operates in synergy with other corporate functions involved in security and data protection management.
Compliance Certifications	The complete list of certifications held by the Processor is available at the following address: https://www.namirial.com/en/company/certifications/

2. TECHNICAL SECURITY MEASURES

TYPE OF MEASURE	DESCRIPTION
Capacity Planning and Performance Monitoring	The Processor implements a continuous process of analysis and optimization of IT resources to ensure adequate performance for the provision of Services and the management of Personal Data. The system includes proactive monitoring of processing capacity, storage, and network bandwidth. Future needs are projected to ensure scalability and operational continuity. Periodic load and resilience tests are conducted to prevent issues due to overloads or usage peaks.
System Security and Hardening	To minimize vulnerabilities and improve IT infrastructure protection, the Processor applies hardening measures to operating systems, application software, and corporate networks. Systems are configured following security best practices to limit exposure to risks. Unnecessary functionalities are disabled, and access to network services is restricted. Configurations are periodically reviewed and updated according to threat evolutions.
Patch Management and Security Updates	The Processor maintains a structured update management process to ensure protection against software vulnerabilities. Security updates are applied promptly based on the severity of the vulnerabilities. Pre-release testing procedures are in place to avoid negative impacts on service continuity. Critical systems are subject to periodic checks to identify any unresolved vulnerabilities.
Network and System Protection	Personal Data is protected by advanced perimeter security and intrusion detection solutions, including: next-generation firewalls for advanced traffic filtering; IDPS (Intrusion Detection & Prevention System) to identify and block suspicious activities; network segmentation to limit propagation risks in case of an attack.
Malware and Cyber Threat Protection	The Processor employs advanced protection tools to mitigate risks from malware and cyber-attacks: regularly updated antivirus and anti-malware to detect and block threats in real-time; sandboxing systems to analyze and isolate suspicious files before execution; threat monitoring to prevent zero-day attacks.
Communication Security and Data Transmission Protection	The Processor adopts advanced security protocols to ensure the integrity and confidentiality of communications: end-to-end encryption to protect data in transit; authentication and digital certificates to verify communication integrity; VPN segmentation and private networks to reduce interception risks.
Physical Protection of IT Infrastructures	Access to premises where Personal Data is stored or processed is subject to enhanced physical security measures: controlled access with badge systems, entry registration, and prior authorization. 24/7 video surveillance and anti-intrusion alarms. Environmental security measures, including fire protection systems, redundancy of electrical and air conditioning systems, UPS, and backup generators to ensure operational continuity. Emergency and disaster recovery procedures, with periodic simulations to test incident response plans.
Credential Management and System Access	To prevent unauthorized access, the Processor implements a strict authentication and credential management system: Multi-Factor Authentication for users with access to personal data and sensitive information; advanced password policy with length, complexity, and

	periodic expiration requirements; immediate revocation of access in case of termination of employment or change of duties.
System Administrator Management	System Administrators, as subjects with elevated privileges, are subject to strict control and monitoring. The Processor maintains an updated and documented list of System Administrators. Administrative activities are tracked and logged with protected and unalterable logs. Periodic audits are conducted to verify the administrators' actions and the correct application of security policies.