

ADDITIONAL CONDITIONS FOR THE PROVISION OF THE CIE AUTHENTICATION SERVICE

1. Value of these Additional Conditions

These additional conditions (hereinafter '**Additional Conditions**') supplement the General Conditions and refer to the CIE authentication aggregation service.

In case of conflict between the General Conditions and these Additional Conditions, the latter shall prevail.

For anything not expressly provided for, reference is made to the Manual, the Decree, the Decree of 23 December 2015 Technical procedures for issuing electronic identity cards' (Gazzetta Ufficiale no. 302 of 30-12-2015) and other provisions in force, as well as the additional documentation indicated in Article 2 Preamble below.

2. Preamble

Namirial S.p.A., following acceptance by the Ministero dell'Interno (hereinafter also referred to as the 'Ministry') of the specific request, has joined the authentication system 'Entra con CIE' (Log in with CIE) as a private aggregator, to allow users to access the services provided by the aggregated entities through the CIE, pursuant to Article 5 of the Decree of 8 September 2022, concerning 'Methods of use of the electronic identity card' (Gazzetta Ufficiale no. 233 of 05.10.2022).

The Decree of 8 September 2022, concerning 'Methods of use of the electronic identity card', Gazzetta Ufficiale no. 233 of 05.10.2022, (hereinafter also referred to as the 'Decree'), Article 5, paragraph 1, provides that the Ministry shall publish the conditions and procedures by which service providers may integrate access to online services with the digital identity issued to citizens and associated with the CIE (hereinafter also referred to as 'CIEId'), in accordance with the provisions of Article 64 of Legislative Decree No. 82 of 7 March 2005 (hereinafter also referred to as the 'CAD').

In implementation of the provisions of Article 5, paragraph 1 of the above-mentioned Decree, the Ministry has adopted the Operating Manual for public and private service providers (hereinafter also referred to as the 'Manual'), which describes the conditions and operating procedures of the federation process for the adoption of the CIEId digital identity as a means of accessing the services provided online by public administrations and private organisations.

The Ministry is meant to be the provider of the CIEId digital identity.

The Poligrafico e Zecca dello Stato (hereinafter also referred to as 'IPZS') refers to the entity used by the Ministry for the proper performance of the functions and/or tasks assigned to it on the basis of the Decree.

The CIE Federation refers to all entities that, under the conditions and procedures set out in the Manual, obtain authorisation to provide access to online services through the CIEId identity.

Service Providers means public and private entities, aggregators and public service managers that directly or indirectly allow natural or legal persons to access online services through the CIEId.

Aggregators means public or private entities that make available the infrastructure necessary to allow aggregated entities to provide their online services through the CIE.

Aggregated entities are public or private entities that make their online services available via the CIE through an aggregator in accordance with the technical and administrative procedures established by the Ministry and following specific agreements signed between the aggregated entity and the aggregator and notified to the Ministry.

3. Subject matter of the Service

These Additional Conditions concern the provision of private services that offer the Aggregate the possibility of making its online services accessible via CIE. The Aggregator performs its service by carrying out the technical authentication function on behalf of the Aggregate and acting as an intermediary between the Ministry and the Aggregate.

4. Specific obligations and warranties of Namirial

Namirial undertakes to perform the services covered by the Agreement with qualified expertise and diligence, in full compliance with the laws and regulations in force applicable to the Service and the terms and conditions of the Agreement, including the conditions and procedures of the federation process for the adoption of the CIEId digital identity referred to in the Decree and the Manual.

Namirial undertakes, in particular, to comply with the provisions contained in the SAML Technical Manual and the Manual published on <https://federazione.servizi.cie.interno.gov.it/> and in the technical rules, drawn up in accordance with the National Open ID Connect Guidelines adopted by AgID and published by the Department for Digital Transformation on <https://docs.italia.it/italia/spid/spid-cie-oidc-docs/it/versione-corrente/index.html>.

In particular, the Aggregator is responsible for taking charge of the issue (phase – reception), then for Incident Verification and management of the assistance request. The Aggregator intervenes in the event of errors relating to access and use of the service, system crashes and authentication procedures, and network issues. The Aggregator's support activities are partly directed by the operator (Ministry), which provides a table describing errors and related solutions, an online FAQ support tool, and a user manual.

The Aggregator undertakes to act as a technological intermediary between the Ministry and the Aggregate Entities.

Namirial undertakes to provide the Ministry with all the information required by the Manual and the regulations referred to therein.

The Aggregator also undertakes to:



Namirial S.p.A.

Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia
amm.namirial@sicurezzaapostale.it | Tel. +39 071 63494
P.IVA, C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426
www.namirial.com



- a) comply with, adapt to and implement all acts, measures, notices or communications sent by the Ministry and/or the Printing Office falling within its sphere of competence and activity, and facilitate the Ministry and the personnel designated by it in carrying out checks, including on the Aggregate;
- b) monitor the correct implementation by the Aggregate of all the obligations provided for in the agreements entered into between the Aggregator and the Aggregate and, in particular, compliance with the provisions of Legislative Decree No. 196 of 30 June 2003, as amended and supplemented, and European regulations in force on data protection, especially with regard to data security, compliance and responsibility towards data subjects, third parties and the Data Protection Authority, informing the Ministry of any particularly critical violations;
- c) keep a record of user accesses over the last 24 (twenty-four) months, in compliance with current legislation on the protection of personal data;
- d) take all appropriate technical measures to ensure the security of data processing and to prevent harmful events (so-called data breaches) in line with the provisions of current legislation, pursuant to Articles 33 and 34 of EU Regulation 2016/679 (hereinafter also referred to as "GDPR")
- e) ensure that recorded events (logs) are marked with a time reference corresponding to the UTC (IEN) time scale referred to in the decree of the Ministro dell'Industria del commercio ed artigianato No. 591 of 30 November 1993, with a difference of no more than one minute;
- f) forward without delay to the Ministry, including in aggregate form, statistical data and reports of malfunctions received from the Aggregates.

In general, Namirial undertakes to perform all the activities provided for in the Manual and the regulations referred to therein that are not expressly assigned to the Aggregate by this Contract.

5. Specific obligations of the Aggregate

The Aggregate undertakes to:

1. communicate to the Aggregator and keep updated the list of qualified services provided online and the technical information requested by the Ministry to allow their use subject to CIE authentication, assuming all responsibility arising from this information obligation;
2. communicate to the Aggregator, for each of the services included in the list, the list of CIE attributes necessary for use, which must be relevant and not excessive in relation to the type and functionality offered by the service, in compliance with the principles set out in Article 5 of the GDPR and with a view to data protection by design and by default pursuant to Article 25 of the GDPR, undertaking, in any case, to limit the request for data to the minimum set necessary for the provision of the service, in line with the provisions of Article 6 of the Decree and in full compliance with the principle of privacy by design and data minimisation. The Aggregate assumes all responsibility for such communication and compliance with the aforementioned provisions of the GDPR;
3. declare to the Aggregator, under their own responsibility and prior to signing this Agreement, that they meet the integrity requirements set out in Decree No. 169 of 23 November 2020 of the Ministry of Economy and Finance and that they have not incurred any of the impediments referred to in Article 5, paragraph 2, of the Decree, so that the Aggregator may fulfil its obligations under this Agreement. No. 169 of the Ministry of Economy and Finance, and that they have not incurred any of the impediments referred to in Article 5, paragraph 2, of the Decree, so that the Aggregator can fulfil its verification obligations in this regard; this provision applies only to Aggregates who are private individuals;
4. allow the Aggregator to verify, every 4 (four) years, that the requirements and circumstances referred to in the immediately preceding point are still met, as well as to facilitate the Ministry and the personnel designated by the latter to carry out similar checks; this provision applies only to Aggregates who are private individuals;
5. inform the Aggregator if the integrity requirements set out in Decree No. 169 of 23 November 2020 of the Ministry of Economy and Finance are no longer met or if the impediments referred to in Article 5, paragraph 2, of the Decree arise, so that the Aggregator may be removed from No. 169 of the Ministry of Economy and Finance are no longer met or if the impediments referred to in Article 5, paragraph 2, of the Decree arise, so that the Aggregator itself can take steps to stop the service used by the aggregated entity and forward a similar communication to the Ministry at the certified email address servizidemografici.prot@pec.interno.it ;
6. adopt the necessary level of security to allow access to its services through CIE authentication;
7. carefully assess the possibility of minors accessing online services based on their age, evaluating whether it is necessary to obtain consent from those exercising parental control;
8. ensure the protection of the personal data of authenticated users;
9. not sell data obtained through authentication processes to third parties;
10. not sell profiling services and/or, more generally, commercial services based on knowledge of personal data acquired during authentication processes to third parties;
11. promptly notify the Aggregator, so that it can inform the Ministry at the certified email address servizidemografici.prot@pec.interno.it, of any malfunction or security incident affecting the authentication system, without prejudice to the obligation to notify the Data Protection Authority, in accordance with the legislation on the processing of personal data, and to the Ministry of any violations of the personal data of the subjects for whom it requests digital identity verification, and also to notify the Data Protection Authority and, where appropriate, to communicate to the data subjects in the event of a personal data breach pursuant to Articles 33 and 34 of the GDPR; immediately inform the Aggregator in the event of detecting abnormal use of a digital identity so that the latter can, in turn, communicate this circumstance to the Ministry that issued it at the certified email address servizidemografici.prot@pec.interno.it;
12. promptly notify the Aggregator of any breaches and intrusions into the personal data of the subjects for whom it requests digital identity verification, so that the Aggregator can notify the Ministry at the certified email address servizidemografici.prot@pec.interno.it no later than 24 hours after becoming aware of the incident.
13. scrupulously comply with current EU and national legislation on the protection of personal data and the provisions of the Data Protection Authority, with particular reference to the principles set out in Article 5 of the GDPR, the lawfulness of processing pursuant to Article 6 of the GDPR, the correct and comprehensive information of data subjects on the processing of their personal data pursuant to Articles 12-14 of the GDPR, respect for the rights of data subjects referred to in Articles 15-23 of the GDPR, data protection by design and by default pursuant to Article 25 of the GDPR, the correct formalisation of the role of its personal data processors pursuant to Articles 4(1)(8) and 28 of the GDPR, the training, instruction and possible designation of its personnel pursuant to Articles 29 of the GDPR and 2-quaterdecies of Legislative Decree 30 June 2003 and subsequent amendments and additions, to the keeping of the register of processing activities pursuant to Article 30 of the GDPR, to the security of processing pursuant to Article 32 of the GDPR, the activities necessary in the event of a personal data breach pursuant to Articles 33-34 of the GDPR, the performance of a data protection impact assessment and any prior consultation with the Data Protection Authority pursuant to Articles 35-36 of the GDPR, the appointment of the data protection officer pursuant to and for the purposes of Articles 37-39 of the GDPR and his/her actual involvement in the protection of personal data being processed with reference to the qualified services



- provided online and accessible via CIE;
- 14. ensure the continuous, regular and secure operation of the service provided;
- 15. carry out information and communication activities towards the user in accordance with the timing and content of the communication defined by the Ministry and/or communicated by the Aggregator;
- 16. comply with, adapt to and implement all acts, measures, notices or communications published by the Ministry and/or IPZS relating to the CIE system and/or communicated by the Aggregator;
- 17. communicate to the Aggregator the technical information requested by the Ministry to enable the use of the services;
- 18. comply with the obligations imposed on the Aggregate by the Manual and any other applicable regulations governing the participation of aggregators in the "Entra con CIE" authentication system;
- 19. forward aggregated data to the Ministry for statistical purposes and, without delay, report any malfunctions;
- 20. immediately notify the Aggregator of any circumstance that may affect the performance of the activities referred to in this Agreement;
- 21. collaborate with Namirial in accordance with the agreed terms and comply with the contractual provisions to enable Namirial to provide the Services in a timely manner;
- 22. use the Services in accordance with the Agreement.

The Aggregate undertakes to comply with each provision issued by the Ministry and/or IPZS, of which it is also informed through Namirial. In the event of non-compliance, the Aggregator assumes all responsibility for any non-compliance by Namirial with the Ministry and the Aggregator's right to terminate the contract pursuant to Article 9 below remains unaffected.

The Aggregate, in compliance with the provisions issued by the Ministry, including the Manual, undertakes to cooperate with the Aggregator by providing all useful information and to carry out the activities necessary for the proper provision of the service by the Aggregator, indemnifying the latter from any liability and possible penalties. If, in the course of its activities, the Aggregates Party detects a possible breach of the regulations relating to the CIE or the obligations arising therefrom, it shall immediately report it to the Ministry, notifying the Aggregator, so that the most appropriate measures can be taken.

6. Information and relations with the user

The Aggregate ensures that Users are fully informed about how the services are provided; in particular:

- a) it informs Users, through specific notices and clear and easily readable information material, of the economic and technical conditions for the provision of services and the necessary information on the processing of personal data, in accordance with Articles 12-14 of the GDPR;
- b) provides Users with adequate information regarding any changes to the methods of service provision;
- c) publishes texts containing the acts governing the provision of services and regulating relations with Users. Any changes that may subsequently become necessary will be included in the existing texts and will be adequately disclosed;
- d) provides appropriate information tools, through the activation of telephone and telematic communication lines, whose proper functioning it periodically verifies, also with reference to the protection of personal data

7. Supervision and sanctions by AgID

By joining the 'Entra con CIE' authentication system for the provision of its services, the Aggregator submits to the Ministry's control activities. 5.2 The control activities referred to in the previous paragraph also extend to the Aggregate insofar as it is competent.

In the event that the Ministry revokes the authorisation to use the 'Entra con CIE' authentication system due to non-compliance with the regulations relating to the 'Entra con CIE' authentication system, with the consequent obligation to pay compensation for any financial and non-financial damage caused to users and interested parties, the aforementioned penalties shall be borne by the Aggregate insofar as it is responsible.

8. Liability of the Parties

In addition to what is already established in the General Conditions, pursuant to these Additional Conditions, the Aggregator is liable for damages resulting from wilful misconduct or negligence in the performance of its activities to users, the Ministry and third parties. It shall also be liable for damages where such damages have been caused in the exercise of its activities, due to failure to meet the requirements or because it has not complied with the instructions issued by the Ministry or provided for in the Manual and the relevant legislation in force. Each Aggregator is liable to the Aggregates Party for any damage directly resulting from its own conduct and/or omissions due to wilful misconduct or gross negligence in the performance of its activities on each Aggregated Party during the user authentication process. The defaulting Aggregator shall also be liable for any damage caused to the User.

Any further and different liability of the Aggregator beyond that contained in this article is strictly excluded.

Similarly, the Aggregate is liable for compensation for damages resulting from wilful misconduct or negligence in the exercise of its activities to users, the Ministry and third parties. It shall also be liable for damages where such damages have been caused in the exercise of its activities, due to failure to meet the requirements or because it has not complied with the instructions given by the Ministry or the Aggregator or the Manual and the relevant legislation in force. The Aggregate shall be liable to the Aggregator for any damage that may be caused to the Aggregator as a direct consequence of its conduct and/or omissions due to wilful misconduct or gross negligence in the performance of the activities incumbent upon the Aggregate as provided for in this Agreement, the Manual and the applicable regulations.

9. Termination of the Agreement

The aggregator's membership of the CIE authentication system shall be valid for five years from the date of authorisation to use the system and shall be tacitly renewed.

The Aggregator retains the right to withdraw from the service at any time, giving at least 15 days' notice to the Ministry in the manner provided for. An aggregator intending to cease its activity is required to notify the aggregated entities, at least 60 days in advance, of its intention to cease its activity as an aggregator. The notification must specify the timing and manner of termination. The communication must also inform the Aggregate of the need to contact another aggregator or to join the CIE federation directly as a Service Provider in order to continue to provide online services



through authentication with CIE. Any termination of membership of the CIE authentication system by Namirial S.p.A. and the Ministry, for any reason whatsoever, including the exercise of the right to withdraw from the service, shall also result in the termination of this Agreement, without Namirial S.p.A. being required to pay the Aggregate any amount by way of compensation, reimbursement or indemnity.

10. Confidentiality

In addition to the provisions of the General Conditions, it is understood that Namirial, in its capacity as Aggregator, shall provide the Ministry with a list of Aggregated entities (name, VAT number/tax code) and, for each of these, their contact details (telephone number, e-mail address and certified e-mail address) for any communications from the Ministry and/or IPZS.

11. Transfer of rights

The Aggregate may not transfer or assign, for any reason, in whole or in part, to third parties the obligations and rights arising from this Agreement, without the prior written authorisation of Namirial.

12. Processing of personal data

The Parties mutually undertake to comply with all obligations arising from EU Regulation 2016/679 and any other regulations applicable to the processing of personal data.

In this context, Namirial has independently organised the processing of personal data arising from the performance of the Service, in accordance with the methods it deems most appropriate for compliance with the regulations and processes underlying the provision of the Service.

The Ministry, as the digital identity manager, and the aggregated entity act, within their respective areas of competence, as independent data controllers pursuant to Article 4(7) of the GDPR.

The Aggregator acts, in relation to the Aggregates Entities, as Data Processor pursuant to Articles 4(8) and 28 of the GDPR and undertakes to scrupulously comply with current European and national legislation on the protection of personal data in the performance of its activities.