PRIVACY ANNEX

PREMISE

1. *DEFINITIONS*

The terms used in this Privacy Annex must be understood exclusively according to the meaning resulting from the definitions specified below and / or according to the further definitions that can be found therein:

- *"Client Administration":* the Administrations and / or other entities or legal persons recipients of the services provided by *Sogei*, also through the *Contract*, which hold the title of *Data Controllers* and for which *Sogei* holds the title of *Primary data processor*. In this case, the Supplier will hold the position of *Sub-Data Processor;*

- *"Contract":* means the contract, including its attachments, stipulated between *Sogei* and the *Supplier*;

- *"Personal Data":* any information relating to an identified or identifiable natural person (interested) as defined in the *Personal Data Protection Regulations* (including data belonging to the particular categories of personal data referred to in Article 9 and relating to criminal pursuant to 10 of EU Regulation 2016/679), made available, transmitted, managed, controlled or otherwise processed by *Sogei* (also on behalf of Sogei's Public Client Administrations).

- *"Director of Execution:* subject to whom the responsibility for the execution phase and the entire technical-administrative process of managing the contract is attributed;

- *"Essential elements of processing":* the elements referred to in art. 28, paragraph 3, first paragraph of the EU Regulation;

- *"Supplier":* the contractor designated as the *Primary Manager or Sub-Manager*, based on the designation made by Sogei as the *Owner or Primary Manager* (i.e. the public administrations that use Sogei for the creation and provision of IT services) or , if the conditions are met, with reference to the activities covered by the Contract, as independent Data Controller.

- *"Security incident":* the security breach that involves the loss, modification, unauthorized disclosure or access to confidential data and / or information (not personal data), the violation and / or malfunction of measures of security, of electronic tools, hardware or software to protect data and information;

- *"Security Measures":* physical, logical, technical and organizational security measures adequate to guarantee an adequate level of security to the risk, including those specified in the Contract, together with its Annexes;

- *"Personal Data Protection Regulations*": all laws, provisions and regulatory directives applicable in relation to the processing and / or protection of Personal Data, as amended from time to time, including, but not limited to, the EU Regulation 2016/679 ("EU REGULATION"), Legislative Decree 196/2003 as amended by the Italian adaptation legislation referred to in Legislative Decree 101/2018, circulars, opinions and directives of the National Supervisory Authority, as well as the guidelines and interpretative measures adopted by the European Data Protection Board.

- *"Persons authorized to process data":* people who as employees, collaborators, administrators or consultants of the *Supplier* have been authorized to process personal data under the direct authority of the *Primary Manager or Sub-Manager or Independent Owner;*

- *"Primary data processor":* the natural or legal person, public authority, service or other body that processes personal data on behalf of the *Data Controller* (i.e. Sogei in the case of data owned by customer administrations or the *Supplier* in the case of data of which Sogei is Data Controller);

- *"Data Protection Officer (DPO)":* the subject designated by the Data Controller pursuant to art. 37 and ss. of the EU Regulation;

- *"Sogei":* SOGEI - Società Generale d'Informatica S.p.A. as *Data Controller* or as the *Primary Data Processor*;

- *"Sub-Data Processor":* the natural or legal person, the public Authority, the service or other body that carries out under a written contract with another *Primary Data Processor*; or the Supplier or the subcontractor / *Sub Data Processor* authorized by SOGEI;

- *"Data Controller":* the natural or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of the processing of personal data; when the purposes and means of such

processing are determined by the law of the European Union or of the Member States, the *Data Controller* or the specific criteria applicable to its designation may be established by the law of the Union or of the Member States; i.e. Sogei and / or the Customer Administrations and or in some cases, if the conditions apply, the Supplier if he can qualify as an *Independent Data Controller;*

- "*Treatment":* any operation or set of operations carried out with or without the aid of automated processes and applied to Personal Data or a set of Personal Data, such as the collection, registration, organization, structuring, conservation, l 'adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or, any other form made available, comparison or interconnection, limitation, alignment or combination, cancellation or destruction;
- *"Violation of personal data (data breach)"*: the security breach that accidentally or illegally involves the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed;

2. *OBJECT*

This document (hereinafter "**Privacy Annex**") **constitutes an integral and substantial part of the Agreement between *Sogei* and the *Supplier*.**

This Privacy Annex is prepared in accordance with the provisions of art. 28 of Regulation (EU) 2016/679 (hereinafter "EU Regulation") and governs the instructions that the Supplier undertakes to observe in the context of the *Processing of Personal Data* that it will carry out in carrying out the activities covered by the *Contract*, ensuring compliance with the current legislation on data protection and security.

As part of the public tender procedure, the *Supplie*r has declared that it is able to ensure suitable and adequate guarantees in terms of specialist knowledge, reliability, resources, also with regard to the adoption of technical and organizational measures to ensure that the *Personal Data* comply with the *Personal Data Protection Regulations*.

By signing *the Contract* and this *Privacy Annex*, which forms an integral part of it, *the Supplier* confirms his direct and in-depth knowledge of the obligations he assumes also in relation to the *Contract* and the provisions of the *Personal Data Protection Regulations*; the Supplier therefore accepts, according to the assignment of the role and the obligations referred to in art. 28 of the *EU Regulation (*hereinafter "appointment" or "designation"), to be designated as *Primary Manager or Sub - Responsible* for the processing of Personal Data unless, with reference to the activities covered by the Contract and the conditions are met, the Supplier, is not an independent data controller.

However, it is understood that where the activities covered by *the Contract* do not involve the processing of *Personal Data* or the Supplier acts as an independent Data Controller, the appointment of the Supplier as Data Processor will be ineffective.

This document also contains the obligations and instructions for the *Processing of Personal Data* that the *Supplier a*nd / or its *Sub-Managers* undertake to observe in the context of the Processing carried out in execution of the Contract, ensuring compliance with current legislation in matter. If the Supplier detects its inability to comply with the conditions and instructions contained in this *Privacy Annex*, even by chance or force majeure, it must implement all possible and reasonable measures to ensure the safety of the Treatments and immediately notify Sogei, agreeing with this '' last any actions and / or further safety and protection measures.

However, it is understood that failure by the *Supplier* to comply with the provisions of the Contract and this *Privacy Annex* will be considered a serious breach and will result in the termination of the Contract and the effects connected to it in accordance with the provisions of the Contract itself.

This appointment will be deemed accepted (i) either when this *Privacy Annex* duly signed is sent to *Sogei*, (ii) or, pursuant to and for the purposes of art. 1327 of the Civil Code, with the fulfillment of the services inherent to the underlying contractual relationship and in any case with the start of the processing activities, regardless of which of the two events occurs first.

It is understood that this Privacy Annex does not apply in cases where the execution of the Contract does not involve, by the Supplier, the Processing of Personal Data or in the event that such Processing will be carried out by the Supplier as independent Data Controller. o under the joint ownership regime with Sogei pursuant to art. 26 of the Regulations, the latter case in which a suitable joint ownership agreement will be entered into between the parties.

3. ROLE OF THE SUPPLIER

The obligations and instructions contained in this *Privacy Annex* are to be considered applicable to the *Supplie*r beyond the role assumed in the *Processing activities* and can be integrated and waived only on the basis of further and specific instructions and / or appointment of *Sogei and / or the Customer Administration*. The subsequent articles, therefore, refer to the obligations assumed by *the Supplier* in relation to the *Processing of Personal Data* related to the execution of the *Contract.*

In the event that it is specified in the Contract, in the related Attachments or in the documents issued by Sogei that, with reference to the activities it contains, *the Supplier* assumes the status of *Independent Data Controller*, the latter undertakes in any case to observe the obligations provided for in the Contract, by the *Personal Data Protection Regulations* and, as applicable, by this *Privacy Annex.*

If it is specified in the Contract, in the relevant Attachments or in the documents issued by Sogei that, with reference to the *Personal Data* processed by the Supplier in execution of the Contract, *Sogei* plays the role of *Data Controller*, the *Supplier* undertakes to observe all the obligations and instructions provided in the Contract and in this Privacy Annex and in the further instructions that will be issued to the same in the technical-functional documents having contractual relevance.

If in the Contract, in the related Attachments or in the documents issued by SOGEI it is specified that, with reference to the Personal Data processed by the Supplier in execution of the Contract*, Sogei* plays the role of *Primary Data Processor*, the *Supplier* will assume the role of *Sub-Manager of the treatment*. In this case, the Supplier undertakes to observe all the obligations and instructions provided for in the Contract and in this Privacy Annex, as well as any further instructions given by Sogei in accordance with what has been received from the Data Controller and which will impose the same on the Supplier. obligations envisaged by Sogei of the Customer Administration with respect to the Processing of Personal Data.

In the **appendix 2),** pursuant to Article 28, paragraph 4 of the *Regulation*, the General Instructions given by the *Data Controller* / *Data Controllers* to *Sogei* as the *Primary Data Processor* and which the *Supplier* is required to observe in the execution of the activities provided for in the *Contract* are reported . It is understood that, in the event of a conflict, the instructions given by the *Holder / Holders* as provided for in the appendix 2) will prevail over those given by *Sogei* with this deed. If the activities referred to in the Contract were carried out by the *Supplier* in favor of several Owners, the General Instructions given by the Owner in whose interest the *Personal Data Processing* activities are carried out will prevail.

Furthermore, with reference to the activities covered by the Contract, the *Customer Administrations* can directly designate the *Supplie*r as the *Primary Data Processor* where the latter is involved in *Personal Data Processing* activities of which the *Customer Administrations are Owners*. In this case, the *Supplier* undertakes to observe all the obligations and instructions for processing contained in the Contract and in this *Privacy Annex*, as well as any further instructions given directly by the Customer Administrations.

However, it is understood that if the activities referred to in the *Contract* do not involve the processing of *Personal Data*, the appointment of the *Supplier* as *Data Processor / Sub-Manager* will be ineffective.

SUPPLIER OBLIGATIONS AND INSTRUCTIONS

I. CODE OF ETHICS

1. The Supplier undertakes to fully comply with the provisions of the Code of Ethics adopted by *Sogei* (present on the website www.sogei.it), undertaking to comply with what is indicated therein, with the sanctions provided for by the *Personal Data Protection Regulations* as well as by the rules of the criminal code as applicable, for all *Personal Data* that *Sogei* or its collaborators should communicate or for news, information or documents relating to the activity carried out by *Sogei* on behalf of the *Customer Administration* which the *Supplier* or its collaborators should become aware in the execution of the activities covered by the *Contract.*

II. SUPPLIER'S OBLIGATIONS

1. The Supplier is authorized to process the personal data necessary for the execution of the activities referred to in the object of the Contract.

2. To this end, the Supplier undertakes to:

- – to ensure full compliance with the contents of this *Annex* as well as in the additional documents as provided for in paragraph II.A) below;

- not determine or favor, through actions and / or omissions, directly or indirectly, the violation by Sogei and/or customer administration of the *Personal Data Protection Regulations*;

- treat the Personal Data exclusively in compliance with the documented instructions of Sogei, to the extent reasonably necessary for the execution of the Contract, and to the *Personal Data Protection Regulations*;

- adopt, implement and update adequate *security measures* to guarantee the protection and security of *Personal Data* in order to preventively and non-exhaustively indicate:

• security incidents and or Data Breach;

• any violation of security measures;

• all other forms of treatment of unauthorized or illegal data.

3. The *Supplier* must comply with all the *Personal Data Protection Regulations*, including those that will be issued during the execution of *the Contract* to ensure an adequate level of security of the *Processing*, including confidentiality, in such a way as to reduce to a minimum the risks of destruction or loss, even accidental, modification, unauthorized disclosure, unauthorized access, even accidental or illegal, or Treatment that is not permitted or does not comply with the purposes of the Treatment.

4. The Supplier undertakes to designate the professional figure of the Data Protection Officer pursuant to art. 37 of EU Regulations and to communicate the relevant data and contacts in a timely manner to Sogei and to the Customer Administration (– in the event that the Owner is a Customer Administration).

II.A) Essential elements of the treatments that the Supplier has been authorized to perform

1. The essential elements of the processing referred to in art. 28, paragraph 3, first paragraph, of the EU Regulation are contained in the Contract, in its annexes, in this Privacy Annex as well as in the appendix 1 of the same.

2. The essential elements of the processing are indicated in a generic way if they refer to any type of personal data and data subjects and may coexist with the indication of more specific (timely) essential elements of the processing if the execution of the contract is envisaged of activities for which the processing of personal data is already known in greater detail.

3. However, it is understood between the Parties that during the execution of the Contract, the essential elements of the Processing may be subject to integration, variation or modification by Sogei or the Owner (in the event that the Owner is a Client Administration).

4. If the essential elements of the punctual processing are not known at the time of signing the Contract, they may be provided later.

5. It is understood that where the Contract provides for the provision of services with the functions of "System Administrator", the Supplier's staff could have access and / or come into contact with some of the personal data present in the Sogei and / or the Customer Administrations. Therefore, the Supplier will be appointed Data Processor or Sub-manager with reference to any processing operations that are co-essential to the performance of the services set out in the Contract and will individually appoint the natural persons who carry out the duties of System Administrator, as specified in paragraph II.B), in accordance with the Provision of the Guarantor for the protection of personal data of 27 November 2008 and subsequent amendments, authorizing them to carry out only the processing operations strictly related to the areas entrusted.

6. The duration of the processing of personal data is limited and coincides with the duration of the contract and its possible extensions and / or specific legal obligations.

II.B) Obligations of the Supplier

The *Supplie*r also undertakes to:

- process only the data necessary for the execution of the activities covered by the Contract;
- immediately inform Sogei and the Data Controller (in the event that the Data Controller is a Client Administration) if he deems that the instructions given to him with this Privacy Annex and / or through additional documents are, or may be, contrary to the relevant Regulations Protection of Personal Data;
- ensure that the processing of personal data is carried out in a lawful, correct, adequate, relevant manner and takes place in compliance with the principles set out in art. 5 and ss. of the EU Regulation;
- ensure the confidentiality of the Personal Data processed for the execution of the Contract activities;
- designate in writing the Persons authorized to process data, promptly identifying the permitted areas of operation. The Supplier must keep an updated list containing all the names of the Persons authorized to process the data and the related authorization and access profiles, with reference to which Sogei and / or the Customer Administration may carry out periodic checks also by means of their own third parties. authorized for this purpose;
- ensure that the Persons authorized to process personal data under this Agreement:
  - **i)** are committed to confidentiality or have an adequate legal obligation of confidentiality;
  - **ii)** have received, and receive, from the Supplier the necessary training on the protection of Personal Data;
  - **iii)** access and process Personal Data by observing the instructions given by the Supplier;
  - **iv)** do not leave the workstation unattended and avoid leaving hardware devices or paper documents containing personal or confidential data unattended;
  - **v)** keep the confidential components of the authentication credentials (password, pin, etc.) that allow the activities to be carried out secret;
  - **vi)** do not use any removable device (CD, DVD, USB device) for storing Personal or confidential data;
  - **vii)** do not extract Personal Data from any "pool" PCs (desktop or portable) or, if this is indispensable according to the activity carried out, they must immediately delete them;
  - **viii)** in the event of disposal of removable media containing Personal or confidential data, they shall be formatted in order to make the Personal Data contained therein unavailable, proceeding, in case of impossibility, to their destruction;
  - **ix)** return any device that contains Personal or Confidential Data and keep any information of which they become aware in the performance of their activities confidential;
- adopt and / or use a suitable system of identification, authentication and authorization of access to Personal Data for Persons authorized to process. The operations carried out by the Authorized Persons must be registered and be available for consultation, also by Sogei and / or by the Data Controller (in the event that the Data Controller is a Client Administration) as part of their supervisory duties, in compliance with the current legislation on remote control of workers (Article 4 of Law No. 300/1970);
- identify and appoint, if the conditions are met, as "System Administrators" the natural persons in charge of the management and maintenance of the systems in accordance with the provisions of the Provision of the Guarantor for the protection of personal data of 27 November 2008 (" Measures and precautions prescribed to the owners of the treatments carried out with electronic tools in relation to the attributions of the functions of system administrator ") and subsequent amendments and additions. In this case, the Supplier must prepare and keep updated a list of these subjects and monitor, where applicable, their related activities in accordance with what is indicated in the provision referred to last. In relation to the control activities of the System Administrator activities, as provided for in the aforementioned provision, the Supplier may request information from Sogei relating to logical access, if not in its direct availability. This constantly updated list must be sent to Sogei in the figure of the Director of Contractual Execution and / or the Owner (in the event that the Owner is a Client Administration);
- ensure that the Persons authorized to process personal data under this Agreement are in possession of the requisites of morality, experience, capacity and reliability required by the Personal Data Protection Regulations;

- if the conditions are met, fulfill the obligations of issuing the information and requesting consent, where necessary, towards the interested parties;
- take into account, in the execution of contractual activities, the principles of data protection from design and protection by default ("privacy by design" and "by default") also with the help of the instructions received;
- provide, upon request, any copy of the Personal Data of employees, administrators, consultants, collaborators or other personnel of the Supplier authorized to process, during the activities covered by the Contract[1] exclusively for purposes relating to the execution of contractual and administrative accounting activities, as well as for the safety of the offices and systems. The Supplier, therefore, authorizes Sogei to extract such Personal Data from its information systems exclusively for the aforementioned purposes.

II.C) Obligations of the *Supplier* in the context of the rights exercised by the *Interested Parties*

1. The *Supplier* must collaborate and support in giving written feedback, even of mere denial, to the requests transmitted by the Interested Parties in the exercise of the rights provided for by the articles 15-23 of the EU Regolations namely the requests for the exercise of the right of access, rectification, integration, cancellation and opposition, the right to limit the treatment, the right to data portability, the right not to be the object of a trial automated decision-making, including profiling.

2. The *Supplier* must provide support, in this activity, so that the reply to the requests for the exercise of the rights of the Interested parties takes place without justified delay, and in any case no later than the useful and / or legal term provided for responding to requests from the interested parties.

3. If the Supplier receives complaints and / or the Interested parties exercise their rights by sending the related request directly to the Supplier, the latter must promptly forward it, and in any case no later than 3 days from receipt, by e-mail to Sogei and / or to the Customer Administration (in the event that the same directly designates the Supplier as the primary data processor).

II.D) Obligations of the Supplier that uses Sub-Data Processors

1. The Supplier may resort to Sub-Managers for the execution of specific Treatments by giving timely communication, and in any case before the start of the processing activities, to Sogei or, where required, to the Data Controller (in the event that the Data Controller is a Customer Administration) the names / company name and the processing activities to be delegated; also undertakes to transmit, where required, the deed of designation of the Sub-Managers. In the event of a request for subcontracting, the commitment to appoint the subcontractor must be indicated in the subcontracting application and must be formalized after the subcontracting authorization issued by Sogei.

2. In the event that the Supplier has designated a Sub-Processor, the Supplier and the Sub-Processor must, in compliance with the provisions of art. 28, par. 4 of the EU Regulation, be bound by a written agreement containing all the data protection obligations provided for in the Contract and in this Privacy Annex, as well as any additional and any documented instructions given by Sogei and / or by the Customer Administration.

3. The instructions given by the Supplier to the Sub-Processors must in any case have the same content and pursue the same objectives as the instructions provided by Sogei and by the Data Controller (in the event that the Data Controller is a Client Administration), with reference to the processing carried out by the Sub -Responsible. In particular, the Supplier guarantees that the Sub-Data Processor ensures the adoption of all Security Measures in accordance with the provisions of the Contract, this Privacy Annex and the Personal Data Protection Regulations and any further instructions. given by Sogei and / or by the Customer Administration.

[1] The Supplier must in turn inform its employees, collaborators, administrators or other personnel that their personal data, in compliance with the principle of relevance, will be communicated to third parties, and in the case that is relevant here to Sogei, for the exercise of activities of the Contract or for the proper exercise of its activities

4. To this end, Sogei and / or the Customer Administration can verify at any time the guarantees and the technical and organizational measures adopted by the Sub-Manager, also by means of audits, assessments, inspections and inspections carried out by their own staff or through subjects third parties authorized for this purpose. In the event that these guarantees are non-existent and / or inadequate, Sogei, in compliance with the contractual provisions, may terminate the Contract with the Supplier.

5. In the event that the outcome of the verifications, inspections, audits and assessments the Security Measures should prove inadequate with respect to the risk or, in any case, unsuitable for ensuring the protection of the data being processed, Sogei will apply a penalty to the Supplier, as contractually provided , and will warn the same to have the Sub-Manager adopt all the most appropriate measures within a reasonable period that will be set if necessary (taking into account the nature, scope of application, context and purposes of the processing, the type of data and the category of interested parties involved as well as the level of risk relating to the data breach, the severity of the breach that has occurred and the security incidents). In the event of failure by the Sub-Manager and / or the Supplier to comply with this warning, Sogei may terminate the Contract and enforce the final guarantee, without prejudice to compensation for greater damage.

6. In any case, Sogei or the Customer Administration remains entitled to oppose the addition or replacement of the Sub-Processor with other Sub-Managers.

7. Should the Sub-Data Processor fail to fulfill his obligations or the instructions received and / or carry out, through actions and / or omissions, Security Incidents and / or violations of the Personal Data Protection Regulations, the Supplier will respond entirely against Sogei and / or the Client Administration, being unable in any way to oppose that said non-fulfillment is due, in whole or in part, to the Sub-Manager.

III. THE SUPPLIER'S TREATMENT REGISTER

1. The Supplier is obliged to prepare, store and update - also with the help of its Data Protection Officer - a **register**, in electronic format, of all the categories of activities relating to the processing (or treatments) performed on behalf of the Data Controller, as required by art. 30, paragraph 2, of the EU Regolation.

2. At the request of the Supervisory Authority, the Supplier will make the Registry available to the Authority itself, at the same time informing Sogei or the Data Controller (in the event that the Data Controller is a Client Administration).

IV. SUPPORT, COLLABORATION AND COORDINATION OBLIGATIONS OF THE SUPPLIER OF TREATMENT IN THE IMPLEMENTATION OF SOGEI'S OBLIGATIONS

The Treatment Provider assists and cooperates in ensuring compliance with the obligations set out in articles 31, 32, 33, 34, 35 and 36 of the EU Regulation, as described below.

IV.A) Safety measures.

1. The Supplier must put in place adequate technical and organizational measures to guarantee an adequate level of security to the risk and guarantee the respect of the obligations of the art. 32 of the EU Regulation. These measures include, among others:

   a) pseudonymisation and encryption of personal data;

   b) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on a permanent basis;

   c) the ability to promptly restore the availability and access of personal data in the event of a physical or technical accident;

   d) a procedure to test, verify and regularly evaluate the effectiveness of the technical and organizational measures in order to guarantee the security of the treatment.

2. The Supplier undertakes to adopt the security measures provided for by sector codes of conduct where they exist and by the certifications where acquired (art. 40 -43 EU Regulation).

3. The Supplier carries out the risk analysis necessary to assess the level of security and the Security Measures necessary for the Processing. In carrying out this analysis, the Supplier must take into account, in particular, the risks presented by the Treatment and which derive, in particular, from the destruction, loss, modification, unauthorized disclosure or access, in an accidental or illegal, from the processing not allowed or not in accordance with the purposes of the processing.
4. The methods for carrying out the aforementioned activities by the Supplier must comply with:
   – the Personal Data Protection Regulations and, in particular, the EU Regulation;
   – Document WP 243 rev.01 - Guidelines on data protection officers (DPO) of 13 December 2016;
   – to Document WP 248 rev. 0.1 - Guidelines concerning the impact assessment on data protection as well as the criteria for establishing whether a treatment "may present a high risk" pursuant to regulation 2016/679 of 4 October 2017.
5. The performance of these activities must also be based on the principles and indications present in the following Standards:
   – Standard ISO / IEC 29134: 2017 Information technology - Security techniques - Guidelines for privacy impact assessment;
   – Standard ISO / IEC 27001: 2013 Information technology - Security techniques - Information security management systems;
   – ISO / IEC 31000: 2018 Standard Risk management - Guidelines.
6. However, it is understood that any reference to the standards and / or guidelines indicated in the previous points 4) and 5) must be understood as referring to the most recent version, if any.
7. In particular, the activities to be carried out must meet the following criteria, however, subject to possible updates and modifications by Sogei:
   a) preliminary analysis of the information of the treatment in question;
   b) identification of the data included in the treatment according to the privacy by default principle, definition of a conceptual model and classification of entities, with regard to confidentiality, integrity and category of personal data;
   c) definition of the activities that make up the Treatment (or functionality in the case of an ICT service);
   d) classification of the processing in terms of privacy characteristics (purpose, lawfulness, interested parties, etc.);
   e) risk assessment for the organization (confidentiality, integrity and availability);
   f) assessment of the necessity and proportionality of the processing in relation to the purposes;
   g) assessment of the risks for the rights and freedoms of the interested party relating to the type of data processed;
   h) assessment of the risks for the rights and freedoms of the interested party relating to the type of treatment, as required by the guidelines WP 248;
   i) in case of need to carry out an impact assessment, identification of specific security measures and relative adequacy assessment;
   j) assessment of the overall intrinsic risk for the processing (for the organization and for the interested party) and identification of suitable security measures according to the principle of privacy by design and relative adequacy assessment in accordance with the standards referred to in the previous point;
   k) drafting of the document containing the risk analysis, the related Security Measures and the relative adequacy assessment to be proposed to Sogei and or to the Owner (in the event that the Owner is a Client Administration) according to the document model defined by Sogei; acknowledgment of any observations by Sogei, the Data Controller, DPO, Privacy Guarantor and Authority.
8. The results of the risk analysis for the identification of adequate Security Measures will be reported by the Supplier in a specific document containing at least the following information: i) identification and classification of Personal Data also processed in terms of confidentiality and integrity; ii) classification of the Treatment also in terms of availability; iii) assessment of the risks for the interested party and inherent in the treatment; iv) identification of the Security Measures as required pursuant to Article 32 of the EU Regulation.

9. The Supplier, pursuant to art. 32, paragraph 4 of the EU Regulation, guarantees that anyone who acts under his authority and has access to Personal Data will not process such data unless duly instructed, unless required by the law of the Union or the Member States.

IV.B) Obligations of the Supplier in the case of "data breach"

1. The Supplier must assist and cooperate fully in the fulfillment activities referred to in Articles 33 and 34 of the EU Regulation.
2. In particular, the Supplier must:

- prepare and update a register containing all violations of personal data and make it available upon request;
- communicate to Sogei and / or to the Data Controller (in the event that the Data Controller is a Customer Administration), immediately and, in any case, without undue delay, any Personal Data Violation since the Supplier, or one of its Sub-Processors, had knowledge of it or had evidence to suspect that a Violation has occurred. This communication must be prepared in writing and contain all the information referred to in art. 33 of the EU Regulation and be sent together with all the necessary documentation to allow Sogei and / or the Data Controller (in the event that the Data Controller is a Customer Administration) to notify, without undue delay, said Violation to the competent Supervisory Authority within and no later than 48 hours from when he became aware of them;
- investigate the breach of personal data by adopting all the technical and organizational measures necessary to eliminate or contain the exposure to risk and collaborate with Sogei and / or with the Data Controller (in the event that the Data Controller is a Client Administration) in the activities of investigation, mitigating any damage or detrimental consequence for the rights and freedoms of the interested parties (so-called "Mitigation measures") as well as implementing, subject to approval by Sogei and / or the Customer Administration, a plan of measures for the timely reduction of likelihood that a similar Violation will recur in the future;
- in the event that Sogei has to provide information (including details relating to the services provided by the Supplier) to the Owner and / or the Supervisory Authority, the Supplier will support Sogei to the extent that the information requested and / or necessary for the Authority control are exclusively in the possession of the Supplier and / or its Sub-Managers.

IV.C) Obligations of the Supplier in the impact assessment.

1. To carry out the impact assessment on the protection of personal data (hereinafter "DPIA"), Sogei and the Data Controller (in the event that the Data Controller is a Client Administration) must consult with their DPO (Article 35, paragraph 2, of the EU Regulation).

2. The Supplier undertakes to assist Sogei and / or the Owner (in the event that the Owner is a Customer Administration), through Sogei, both at a technical and organizational level, in carrying out the DPIA, as governed by art. 35 of the EU Regulation, in all cases in which the processing provides for, requires or requires the performance and / or updating of the same.

3. The results of the DPIA, also for the identification of the necessary Security Measures, will be reported by the Supplier in the risk analysis document referred to in the previous art. IV.A) of this Privacy Annex.

4. The Supplier will provide its assistance in the prior consultation of the Supervisory Authority pursuant to art. 36 of the EU Regulation by providing all the information necessary for

V. ADDITIONAL GUARANTEE OBLIGATIONS OF THE TREATMENT PROVIDER

1. The Supplier undertakes to adopt all the necessary Security Measures and to carry out all the training, information and updating activities reasonably necessary to ensure that the Processing always concerns accurate, correct and updated Personal Data - even if the Processing consists in mere custody o data control activity - performed by the Supplier or by its Sub-Managers.

2. The Supplier undertakes to transmit all the information and documentation that Sogei and / or the Owner (in the event that the Owner is a Customer Administration) may reasonably request from him during the execution of the Contract to verify compliance by the Supplier or of its Sub-Data Processors, of the provisions of the Contract, of this Privacy Annex and of the Personal Data Protection Regulations and of the instructions received, also in terms of Security Measures.

3. The Supplier guarantees the possibility that control and evaluation activities, including through inspections and inspections, of the Personal Data Processing activities carried out by the same Supplier, including therein, can be carried out at the same, also by means of authorized third parties and with reasonable notice. the work of any system administrators, in order to verify compliance with the Contract, with this Privacy Annex and with the Personal Data Protection Regulations and with the instructions received. The Supplier must make available, without any delay and / or omission, all the information necessary to demonstrate its compliance with the aforementioned obligations. In the event that, as a result of these checks, the Security Measures are inadequate and / or unsuitable to ensure the application of the Personal Data Protection Regulations, Sogei will apply the penalties provided for in the Contract to the Supplier, warning him to adopt the necessary measures within a reasonable period that will be fixed if necessary (taking into account the nature, scope of application, context and purposes of the processing, the type of data and the category of interested parties involved as well as the level of risk of violation and / or the seriousness of the violation that has occurred). In the event of failure by the Supplier to comply with this warning, Sogei may terminate the Contract and enforce the definitive guarantee, without prejudice to compensation for greater damage.

4. The Supplier must immediately inform and assist Sogei and / or the Owner (in the event that the Owner is a Customer Administration) in case of inspections, of any measures taken against him or in case of procedures before the Authorities for the protection of personal data, national and European, and / or to the Judicial Authority in relation to the Treatments assigned to it and unless such communication is prohibited by the provision or by law.

5. In such circumstances, unless prohibited by law, the Supplier must**: i)** inform Sogei and / or the Owner (in the event that the Owner is a Customer Administration) promptly, and in any case no later than 24 hours from receipt of the request for ostension; **ii)** collaborate with Sogei and / or with the Data Controller, in the event that they intend to legally oppose such communication; **iii)** guarantee the confidential treatment of such information.

6. The Supplier acknowledges and acknowledges that, in the event of a violation of the Personal Data Protection Regulations as well as the provisions of this Privacy Annex, in addition to the application of the clauses relating to the termination of the Contract, the related penalties and any compensation for greater damage, however, without prejudice to Sogei's right to resort, even judicially, to precautionary, injunctive and summary measures or other equitable remedies, in order to immediately interrupt, prevent or limit the processing or any use and disclosure of Personal Data.

7. The Supplier undertakes to hold Sogei and the Owner harmless and harmless (in the event that the Owner is a Customer Administration) from any material, immaterial and reputational damage, direct or indirect, as well as from any cost, expense (including legal fees), burden, interest and / or sanction that the latter should suffer as a result of the non-fulfillment of the obligations assumed with the Contract and with this Privacy Annex by the same, by its Sub-Managers or by its agents, employees, collaborators, as well as of any other person appointed by it to perform the services set out in the Contract.

VI. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

1. In compliance with the provisions of EU / 2016/679 Regulation, the Supplier must ensure that the personal data being processed will be managed within the EU and that no transfer of the same will be made to a third country or organization. international outside the EU or the European Economic Area, with the exception of the countries / territories / organizations covered by an adequacy decision made by the European Commission pursuant to art. 45 EU / 2016/679 Regulation or other adequate guarantees pursuant to art. 46 and ss. of the Regulation itself (eg use of the binding corporate rules Binding Corporate Rules - BCR) as well as the adaptation to any additional additional measures referred to in the recommendations of the European Data Protection Board. Apart from the aforementioned exceptions, the Supplier must ensure that any platforms / servers on which the aforementioned data transit are based in the EU and that any replication of the data is not transmitted outside the EU or the European Economic Area. In the case of remote assistance / maintenance services whose performance still involves the transfer

outside the EU of data paths connected to the service itself, any personal data contained in the path must be appropriately anonymized by the Supplier.

2. If, as a result of any checks, inspections and audits carried out by Sogei and / or by the Data Controller (in the event that the Data Controller is a Client Administration), non-EU data transfers should result in the absence of adequate guarantees and any further measures above, the Supplier will be warned against the immediate interruption of the unauthorized data transfer. In case of non-compliance following the warning, also made pursuant to art. 1454 of the Italian Civil Code, Sogei will notify the Privacy Guarantor and may, due to the seriousness of the Supplier's conduct and without prejudice to the possibility of setting a further deadline for compliance, terminate the implementation contract and enforce the definitive guarantee, without prejudice to compensation of the greatest damage.

VII. OBLIGATIONS OF THE SUPPLIER AT THE END OF THE CONTRACT.

1. At the end or termination of the Processing for any reason, the Supplier undertakes, for itself and also for its Sub-Managers, not to keep and destroy in a secure manner all data processed in execution of the Contract, deleting all existing copies in its possession, except in cases where the conservation of the same is required to fulfill legal obligations.

2. The Supplier and its Sub-Managers must document such cancellation in writing. The Supplier, upon request, will issue a specific written declaration containing the attestation that at the same or at its Sub-Managers there is no copy of data and / or information that they have come into possession of in execution of the Contract, except those whose conservation is necessary by virtue of the applicable legislation. Sogei and / or the Owner (in the event that the Owner is a Client Administration) reserve the right to carry out checks and verifications aimed at ascertaining the veracity of said declaration.

VIII. CHANGES IN THE LAWS RELATING TO THE TREATMENT OF PERSONAL DATA.

In any case, if, during the term of the Contract, a modification of the Personal Data Protection Regulations should occur that determines the need for further compliance also in terms of security measures, the Supplier will collaborate with Sogei and with the Owner. (in the event that the Data Controller is a Client Administration), within the limits of its resources and its technical-organizational skills, so that corrective adaptation measures necessary for the fulfillment of the services inferred in the Contract are developed, adopted and implemented.

APPENDIX 1

ESSENTIAL ELEMENTS OF THE TREATMENT

to be filled in by Sogei

For essential elements of the treatment referred to in art. 28, paragraph 3, of the GDPR means, with reference to the Contract, the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the Data Controller.

Most of these elements can be deduced from the Contract and its annexes and, therefore, only the essential elements not deductible from this documentation are disclosed below, namely the nature and purpose of the processing, the type of personal data processed, the categories of data subjects.

The essential elements of the processing are indicated in a generic way if they refer to any type of personal data and data subjects and may coexist with the indication of more specific (timely) essential elements of the processing if the execution of the contract is envisaged of activities for which the processing of personal data is already known in greater detail.

[*Se sono noti i Trattamenti/Servizi Ict/Servizi tecnici sui quali il fornitore è chiamato ad operare specificarli di seguito. Gli ulteriori campi possono essere compilati sulla base di quanto previsto nel documento IS-31-PR-04 - Glossario GDPR.*

Si precisa che tali elementi vanno altresì indicati in fase di affidamento delle attività nel caso in cui all'atto della stipula siano stati dati al fornitore «Elementi essenziali del trattamento» generici e non puntuali ovvero nel corso dell'esecuzione contrattuale siano individuati nuovi elementi essenziali del trattamento "puntuali" rispetto a quelli già comunicati]

It should be noted that for the purposes of carrying out the activities provided for in the aforementioned Agreement, this Company is authorized to operate, in the context of the Treatments / ICT Services / Technical Services listed below:

- As Responsible, that is, if the treatments are carried out for Sogei *[INSERIRE SOLAMENTE I TRATTAMENTI DI SOGEI TITOLARE es TR-0001 – Eliminare la sezione se non compilata*]

Sogei Owner - Essential elements of the treatment - Punctual						
Treatment identifier	**Treatment description**	**Nature of the treatment**	**Purpose of the processing**	**Subcategories of Personal Data**	**Categories concerned**	**For whom the treatment is carried out**

- as Sub-responsible, that is, if the treatments are carried out on behalf of the client administrations (*INSERIRE SOLAMENTE I Sercvizi Ict/Servizi tecnici DI SOGEI RESPONSABILE es ENT-SA-0001 – Eliminare la sezione se non compilata*)

Sogei Responsible - Essential elements of the treatment - Punctual						
Treatment identifier	**Treatment description**	**Nature of the treatment**	**Purpose of the processing**	**Subcategories of Personal Data**	**Categories concerned**	**For whom the treatment is carried out**

[*Se gli elementi essenziali del trattamento non sono noti ma si presume che il contratto implichi un trattamento di dati personali specificare quanto segue: In caso contrario eliminare il paragrafo*]

Essential elements of the treatment - Generic				
Nature of the treatment	**Purpose of the processing**	**Macrocategories of Personal Data**	**Categories concerned**	**For whom the treatment is carried out**
Automated and / or non-automated	*Inserire la descrizione sintetica dell'iniziativa (rif. campo Anagrafica dell'iniziativa sulla PdA)*	General and specific personal data relating to criminal convictions and offenses	Citizens, employees and contractors	Sogei and / or customer administrations (*specificare la denominazione di tutte le amministrazioni clienti per conto delle quali il fornitore potrà trattare dati personali)*

APPENDIX 2

INSTRUCTIONS IMPOSED TO THE SUB-MANAGER OF THE TREATMENT PURSUANT TO ART. 28, PAR. 4 OF THE REGULATION

In addition to the provisions of the Privacy Annex and by virtue of the role of Sub-Manager of the processing acquired by the Supplier as part of the execution of the Contract, this Appendix contains the directives, instructions and obligations imposed on Sogei by the Data Controller regarding the protection of Personal Data and to which the Supplier must comply in accordance with the provisions of art. 28, parr. 2 and 4 from the aforementioned Privacy Annex.

GENERAL INSTRUCTIONS

1. COMMON ELEMENTS

1.1 The Sub-Processor is authorized to process, on behalf of the Client Administration, all Personal Data owned by the latter and necessary for the proper execution of the Contract, excluding unauthorized treatments and in any case additional to those exclusively necessary for the execution of the task entrusted to him. The essential elements of the processing are listed in the Privacy Annex.

1.2 The Sub-Processor undertakes to comply, within the limits of the obligations assumed by signing the Contract and the provisions of the Regulations, the general and specific instructions contained in this Appendix or communicated in writing at a later time, in this regard, also binding the persons authorized to process the processing and any Sub-Responsible suppliers in the event that this becomes necessary. The Data Controller, also through Sogei, will notify the Sub-Manager of any changes that may be necessary in the processing operations. The Sub-Processor and the persons authorized by the same to process the processing will not be able to carry out any processing operations other than those assigned to him and any changes requested in writing by the Data Controller or, upon indication of this, by Sogei.

1.3 The Sub-Processor, also in accordance with what is indicated in the Privacy Annex, implements the appropriate technical and organizational measures to guarantee a level of security commensurate with the risk presented by the Treatment, in compliance with the provisions of the Contract and based on the needs of the Owner, in particular of destruction, loss, modification, unauthorized disclosure or access, accidental or illegal, of such Personal Data when transmitted, stored or otherwise processed.

1.4 The Sub-Processor, including anyone acting under his authority and having access to Personal Data, is required to keep the information acquired during the performance of activities on behalf of Sogei and in favor of the Data Controller confidential.

1.5 The validity of these instructions and the authorization to carry out the Personal Data Processing in favor of the Data Controller coincides with the duration of the Contract, or its possible extensions, without prejudice to the fulfillment of specific legal obligations or further documented instructions given to the Sub data Processor.

2. **OBLIGATIONS OF THE SUB-PROCESSOR**

2.1 The Sub-Processor, without prejudice to the provisions of the Privacy Annex, must:

- process Personal Data exclusively for the performance of the services provided for in the Contract and for the related purposes, as well as in a lawful, correct, transparent manner and in compliance with all the principles set out in art. 5 of the regulation;
- process Personal Data in accordance with the general and specific instructions given by the Data Controller and / or by Sogei;
- inform Sogei of any request received for any reason directly from the Data Controller;
- process Personal Data only on the documented instruction of the Data Controller or, upon indication of the latter, by Sogei, even in the event of the transfer of Personal Data to a Third Country or an international organization, unless required by Union or national law which the Sub Processor is subject; in this case it is required to inform Sogei about this legal obligation before processing, unless the law prohibits such information for relevant reasons of public interest;
- immediately inform Sogei and / or the Data Controller if it deems that an instruction violates the Personal Data Protection Regulations, or has become impossible to comply with it, adopting any possible and reasonable temporary safeguard measures, as well as agreeing on any and further measures of protection;
- promptly and without undue delay inform Sogei and / or the Data Controller in the event of inspections or requests for information and documentation from the Supervisory Authority in relation to the Processing activities entrusted to the Sub-Manager;
- lend its assistance to the Data Controller, from a technical point of view, for the fulfillment of the existing obligation of the latter pursuant to Articles 13 and 14 of the Regulation;

- fulfill the obligations set out in art. 30, par 2 to 4 of the Regulation, in relation to the processing activities carried out on behalf of the Data Controller and any specific legislation applicable to the data being processed. The Sub-Manager ensures the consistency of his register with that of Sogei and the Data Controller, as well as makes it available to the Supervisory Authority, where required, while at the same time informing the Data Controller and Sogei;
- throughout the execution of the Contract, support the Data Controller, also through Sogei, in taking into account the principles of data protection from the design stage and protection by default, also in the context of application development / MEV and infrastructural services from the start requirements analysis;
- support Sogei in sending, also on behalf of the latter, to the Owner of any document requested by the latter for the execution of the services covered by the Contract, as well as collect, record, organize, consult and possibly delete and destroy Personal Data processed for the purposes and performance of the activities provided for in the Contract itself;
- if the Contract concerns the supply of an ICT Service, proceed, in compliance with the methods and obligations provided for by it, to periodic updates of the operating systems and computer programs aimed at preventing the vulnerabilities of the electronic tools through which it is performed the Treatment and and to correct defects, also identifying those most suited to the types of data and the processing operations that can be performed with them, according to the indications, policies and guidelines defined by the Data Controller and Sogei regarding information security.

2.2 With specific reference to the identification and education of persons authorized to process the processing, the Sub-Manager must:

- provide that they act in accordance with the scope of operations permitted on the basis of the agreements in place, being able to carry out operations functional to the implementation and management of the activities assigned, without carrying out Personal Data Processing that is not necessary or functional with respect to the purposes pursued and duties performed;
- allow him to access the electronic databases and / or the Data of the Owner solely and exclusively for the execution of the commissioned tasks, including the reasons for the safety, operation and maintenance of any systems covered by the Contract. Persons authorized to process may not remove computer media containing Personal Data without express and prior authorization;
- ensure that these subjects do not create new databases without express authorization and maintain absolute confidentiality on the personal data known, even incidentally, by reason of the exercise of the functions assigned to them. To this end, the Sub-Processor guarantees that the persons authorized to process the processing operating under his authority are committed to confidentiality or have an adequate legal obligation of confidentiality;
- provide them with the necessary training on the protection of Personal Data and take all necessary measures so that they can have full knowledge of the instructions given to them;
- ensure that those authorized to process the processing comply with the instructions given to them and the technical and organizational measures prepared, as well as call them to comply with the aforementioned instructions in the event of any violations or whenever this becomes necessary;
- at the request of the Data Controller, make available a list of persons authorized to process.

3. **PROVISION OF DATA TO THE CONTROLLER**

3.1 If the Data Controller or person / function appointed by it needs to access Data not available through the application services for the performance of its institutional tasks, these may be requested in writing from the Sub-Processor, specifying the type of data, the timing and the method of supply. The Sub-Processor is required to make such data available, if necessary, according to guidelines to be agreed.

3.2 Any requests for the provision of data and the relative responses are exchanged through registered communications. The Sub-Processor is informed about the subject / s authorized to request the aforementioned provision of the Data, with any scope limitations.

4. APPOINTMENT OF SYSTEM ADMINISTRATORS

4.1 The Sub-Processor, without prejudice to the provisions of the Privacy Annex, must:

- To identify the System Administrators and comply with the requirements contained in the Provision of the Guarantor Authority for the protection of personal data of November 27, 2008 and subsequent amendments as they are compatible with the Regulations until new issue or revocation by the Authority itself;
- formally and in a traceable manner to authorize the System Administrators, giving them adequate instructions in relation to the activities carried out on the systems and on the Data, taking into consideration the areas of operation allowed to them based on the authorization profile;
- to supervise compliance with the instructions given to System Administrators, supervising the operations entrusted to them on the basis of the areas of operation permitted by the authorization;
- to keep and to keep updated a list of System Administrators that summarizes the functions and areas of operation permitted;
- to keep secret and to guard the authentication credentials assigned to authorized natural persons used for access as System Administrators;

- to verify, even on a sample basis and at least annually, the work of the System Administrators in order to: **(i)** ascertain the maintenance of the subjective requirements for carrying out the tasks entrusted to them; **(ii)** verify the compliance of their work with the Security Measures put in place for the Processing of Personal Data;
- to adopt, within the limits of the obligations established by the Contract, a suitable system of identification, authentication, authorization of any type of access of the System Administrators. Access to data and operations carried out by System Administrators must be tracked and accessible by the Sub-manager, the Owner and / or Sogei as part of their supervisory and audit tasks. Records of data access must: (**i)** have characteristics of completeness, inalterability and the possibility of verifying their integrity; **(ii)** understand the time references and the description of the event that generated them; (**iii)** be adequate to achieve the verification purpose for which they were requested; (iv) be kept for an appropriate period of time in any case not less than six months.

5. SUPPORT AND COLLABORATION OF THE SUB PROCESSOR

5.1 Taking into account the nature of the processing and the information available to it, the Sub-processor, within the limits and in accordance with the provisions of the Contract and the instructions contained in the Privacy Annex, provides his assistance to ensure compliance with the obligations set out in Articles from 32 to 36 of the Regulation.

5.2 The Sub Processor cooperates with the DPOs designated respectively by the Owner and by Sogei in carrying out the tasks referred to in art. 39 of the Regulation.

5.3 The Sub-processor must also:

- To cooperate to provide all the information, data and documentation necessary for the Data Controller to comply with the requests of the Supervisory Authority, or if information is required in the event of audits, pre-litigation and litigation procedures. In such cases, the economic charges related to the fulfillment of the requests cannot be charged either to the Owner or to Sogei;
- not to disclose the Personal Data object of the Processing, meaning the disclosure of the same Data to indeterminate subjects, in any form, including by making them available or consulting;
- not to communicate the Personal Data being processed without the explicit authorization of the Owner, without prejudice to the particular confidentiality requirements expressly specified by the Judicial Authority;
- to assist Sogei and / or the Data Controller to develop strategies to contrast and mitigate risks aimed at reducing, eliminating or accepting the risks identified in relation to a Treatment. These strategies must take into account the context where the Processing takes place, the categories of Data and Data Subjects, as well as the Processing carried out and the related technological progress;
- to agree, upon request, a systematic verification and control plan for compliance with the general and specific instructions given in relation to the Processing of Personal Data carried out in favor of the Data Controller. The Sub-processor provides evidence of the implementation of the plan by means of an annual report, where required;
- to take into account the principles of data protection from the design stage and by default, even in the event of requests for evolutionary maintenance of the systems and applications covered by the Contract on which the Sub-Manager is authorized to operate.

6. SUB-DATA PROCESSORS

6.1 For the execution of the activities provided for in the Contract, the Sub-Processor, where necessary, may resort, pursuant to art. 28, par. 2 of the Regulations, to other Sub-Processors. In this case, the Sub-Processors must comply with the obligations imposed by the Personal Data Protection Regulations and contained in this Appendix, as well as in any further instructions provided by the Data Controller at a later time.

6.2 The Sub-Processor informs Sogei about any changes regarding the addition or replacement of any Sub-Processors involved in the Treatment, thus giving Sogei the possibility to oppose this modification and, in accordance with the instructions received from the same, to communicate them to the Data Controller processing so that it can oppose these changes by providing specific reasons within 15 working days by certified e-mail or registered letter with return receipt. In the absence of opposition, the proposed changes / replacements will be considered approved.

6.3 Without prejudice to the provisions of the Privacy Annex, if the Sub-Processor fails to fulfill its data protection obligations, the initial Sub-Processor retains full responsibility towards Sogei.

***7.* RIGHTS OF THE INTERESTED PARTIES**

7.1 Where required, the Sub-Processor, without undue delay, must assist the Data Controller in giving written feedback, even if of mere denial, to the requests sent by the interested parties for the purpose of exercising the rights provided for in Articles from 15 to 23 of the Regulation, that is to say to the relative requests for the exercise of the right of access, rectification, integration, cancellation and opposition, right to limitation of treatment, right to data portability, right not to be subject to an automated decision-making process, including profiling.

7.2 If the interested parties send the aforementioned requests to the Sub-Manager, the latter must promptly forward them to Sogei, so that the latter, in turn, can promptly forward them to the Owner. It is understood that the Sub-Manager will provide any assistance necessary to meet the obligation to follow up on requests for the exercise of the rights of the interested parties within the terms of the law.

8. SECURITY MEASURES

8.1 To reduce and keep as much as possible the risks and dangers deriving from the *Processing* of *Personal Data* , the *Sub-Manager* undertakes to identify the most appropriate technical and organizational measures to be implemented on the basis of the information received, in such a way that that the *processing* meets the requirements of the *Regulation* and

guarantees the protection of the rights of the data subjects. The *Sub-Manager*, on the basis of the provisions of this Appendix and the additional instructions and methodologies shared with the same, adopts all the *Security Measures* required by art. 32 of the *Regulation*, also ensuring the adoption of all the *Security Measures* provided for by the *Contract*, by the *Privacy Annex* and by the additional *Personal Data Protection Regulations* , also taking into consideration the applicable *best practices* on the subject and the provisions of the National Supervisory Authority and European.

8.2 The *Sub-Manager* undertakes to update the computer network protection systems and systems interconnection systems, also identifying those most suitable for the need to avoid unauthorized access, illegal processing and prevent any loss of *Personal Data* .

8.3 The *Sub-Processor* , in assessing the adequate level of security, undertakes to take particular account of the risks presented by the *Treatment* that derive, in particular, from the destruction, loss, modification, unauthorized disclosure or accidental or illegal access to personal data transmitted, stored or otherwise processed. The *Sub-Manager* also undertakes to define an IT security plan designed to monitor the data and systems, which will take into account the organizational and technical measures necessary according to the types of data being *processed.*

8.4 If the *Contract* envisages the development and evolution of ICT services to be carried out on behalf of the *Owner* , the *Sub-Manager* , on the occasion of the delivery of the documentation contractually provided for at the end of the requirements analysis phase, will deliver to *Sogei* a specific document containing the risk assessment for the relative approval by the *Data Controller* , with particular regard to the rights and freedoms of the data subject and the consequent "security measures for the protection of the service", also including the *Security Measures* resulting from the impact assessment, where necessary , subject to evaluation and approval.

8.5 The *Sub-Manager* must provide for monitoring and auditing activities with the aim of perfecting or in any case improving the countermeasures adopted, in order to measure their effectiveness in the medium and long term.

9. VIOLATION OF PERSONAL DATA ("DATA BREACH")

9.1 The *Sub data Processor* is aware of the obligations imposed on the *holder of the treatment*, in accordance with articles. 33 and 34 of the *Regulation*.

9.2 The *Sub-Manager* undertakes to communicate to *Sogei* and the *Data Controller* any known or even suspected violation of *Personal Data* pursuant to and within the terms provided for in Articles. 33 and 34 of the *Regulation*. To this end, the *Sub-Manager* must comply with the notification flows of the data breach contained in the specific instructions at the bottom of this Appendix, making available - without undue delay and, where possible, within 36 hours of the discovery of the event - any timely and useful information for the correct fulfillment of the obligations deriving from the last mentioned regulations. Once the reasons for the *violation* have been defined, the *Sub-Manager* , in agreement with the *Owner* , *Sogei* and / or another person indicated by them, will take steps to implement as quickly as possible all the *Security Measures* aimed at stemming the occurrence of a new violation of the same kind by any means and resources deemed necessary for the purpose.

9.3 The *Sub-Processor* ensures maximum collaboration to investigate all the necessary and useful aspects to identify the violation and undertakes to implement all the possible additional actions and measures indicated by the *Data Controller*, also through *Sogei* , to deal with the *Violation of personal data.*

9.4 The *Sub-Processor* maintains accurate documentation of all recorded *Personal Data Breaches,* including the circumstances relating to them, their consequences and the measures taken to remedy them. This documentation is integrated with any actions taken by the same and appropriately communicated to the *Owner* and to *Sogei.*

9.5 It is mandatory to maintain absolute confidentiality on the *violations of personal data that have* occurred. This information must not be disseminated in any way in any form, including by making it available or consulting. The communication of the violation is allowed only between the *Owner*, *Sogei* and another person indicated by them and the *Sub-Processor*, without prejudice to those communications required by law or by public authorities.

10. IMPACT ASSESSMENT ("DPIA")

10.1 The *Sub data Processor* is committed to assist the *Holder*, technical and organizational level, in the performance of DPIA, as well as governed by art. 35 of the *Regulation*, in all cases in which the *processing* provides for or requires a preliminary impact assessment on the protection of personal data or its updating.

10.2 The *Sub-Processor* must possibly operate in compliance with any further instructions and / or methodologies approved by the *Data Controller* or shared by the latter with *Sogei*, providing the latter with any information useful for the correct fulfillment of the obligations pursuant to art. 35 of the *Regulation*. The *Sub- Data Processor* also undertakes to assist the *Data Controller* in the preventive consultation of the Supervisory Authority provided for by art. 36 of the *Regulation*.

11. AUDIT

11.1 The *Sub Processor* undertakes to respect the same obligations assumed by *Sogei* towards the *Owner*. To this end, the *Sub-Processor* accepts and acknowledges that the *Data Controller* has the right to analyze, verify or assess compliance by him with the legal and contractual obligations to the *Sub-Processor* in the execution of the *Contract* , where deemed appropriate or necessary. These activities may be carried out upon agreement on the times and methods and in any case with a minimum notice of 3 (three) working days, also taking into consideration the impacts that such activities may have on the correct provision of the services covered by the *Contract.*

11.2 These activities may be carried out by the *Owner* directly using its own internal structures, also with the possible support of external resources or by companies / third parties of its own trust specifically appointed and bound by confidentiality agreements. To implement the above, the *Sub-Manager* undertakes to offer the utmost cooperation in order to allow them (or the company / third party designated and previously communicated to the Sub- *Manager*) to effectively carry

out their audit activity on the *Treatment* , which must always take place in the presence of the *Sub-Manager's staff* and with the drafting of a report signed by the parties.

11.3 During the audit activities, the *Data Controller* will have the right to access the *Sub-Manager's* premises, directly or through specifically appointed persons, whose names will be previously communicated to the latter and to have a copy of all data, documents, information, elements , content of any kind and nature that may be necessary for the performance of the audit on the processing of *personal data.*

11.4 Any non-compliance attributable exclusively to the *Sub-Processor* relating to **(i)** the obligations set out in this document, **(ii)** the applicable law, **(iii)** the policies or procedures envisaged and previously communicated to the *Sub-Manager* , which may arise during the '' audit activity, without prejudice to all rights, including compensation for damage and the hypotheses of co-responsibility indicated by the legislation, by this appointment and by the provisions of the Supervisory Authority, must be resolved by the *Sub-Manager,* bearing the related costs and charges and in any case within an appropriate term agreed from time to time with the *Data Controller,* taking into account the necessary technical implementation times. After the solution of any non-conformities found, the *processing* activities must be perfectly compliant with the obligations assumed by the *Sub-Manager* and the applicable law.

11.5 If the result of the aforementioned checks it is found that the *Sub-Processor* has not complied with the obligations assumed regarding data protection, the instructions received, or has not implemented, in whole or in part, the measures put in place to protect of the *Treatments* and the activities entrusted to him, the *Sub-Manager* , on the recommendation of *Sogei* and / or the *Data Controller* , undertakes to take all necessary measures and to behave in accordance with the instructions received within a reasonable time jointly set if necessary. In the event of persistent non-compliance and / or compliance with the instructions received, the *Sub-Manager* accepts that *Sogei* may replace him based on the seriousness of the non-fulfillment and the contractual obligations it has assumed towards the *Owner.*

12. RETENTION, CANCELLATION AND DESTRUCTION OF DATA

12.1 The *Personal Information* subject to *processing* by the *Sub-Processor* will be kept for the entire lifetime of the *contract.*

12.2 Once the provision of the services covered by the *Contract has been completed* , the *Data Controller* , also through *Sogei* , may request the *Sub-Manager* at any time to cancel and / or return all *Personal Data* subject to *processing* , or to cancel all existing copies, unless Union law or national law provide for data retention pursuant to art. 28 par. 3, lett. g) of the *Regulations.*

12.3 The replacement or disposal of structures, systems and equipment that involve or may involve the cancellation of *Personal Data* must take place on the basis of a specific procedure agreed with the *Data Controller* , without prejudice to the *Personal Data Protection Regulations* and the provisions in force. , as they are compatible with the *Regulation* . Any cancellation of *Personal Data* for which the cancellation terms and / or criteria have not been established can take place with the explicit authorization of the *Data Controller* , also through *Sogei.*

12.4 Any operations to return *Personal Data* must be agreed with *Sogei* , according to the operational and security methods agreed by the latter with the *Data Controller* . The return must in any case be accompanied by the destruction of all copies existing in the information systems of the *Processor.*

12.5 In any case, once the data owned by the *Client Administration* are destroyed or deleted, the *Sub-Processor* must document in writing such destruction or cancellation.

13. RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA

13.1 The *Sub-Processor* communicates to the *Data Controller* and to *Sogei* the name and data of his designated DPO in accordance with art. 37 of the *Regulation.*

14. CODES OF CONDUCT

14.1 In the event that the *Sub-Processor* adheres to a code of conduct approved pursuant to art. 40 of the *Regulation* or to a certification mechanism approved pursuant to art. 42, this adhesion can be used as an element to demonstrate the sufficient guarantees referred to in par. 1 and 4 of art. 28 of the *Regulation.*

15. RESPONSIBILITY

15.1 Failure to comply with the general and specific instructions contained in this Appendix, including those relating to the appointment of the *Sub-Processor*, even after the dissolution or termination of the effectiveness of the *Agreement* for any cause due and / or subsequent to the revocation of this appointment, may entail the consequences for the *Sub-Manager* pursuant to art. 82 to 84, as well as those provided for by art. 28 par. 10 of the *Regulation.*

16. REGULATORY CHANGES AND ADDITIONS

16.1 In the event of changing the *rules on personal data protection* which imposes new requirements - including new physical measures, logic, technical and organization in the field of security *Processing* of *Personal Data* on - *Sub-Processor* supports *Sogei* and *Holder* in identifying the need for adjustments and development, adoption and / or implementation of corrective measures and in adopting, with possible revision of contractual agreements and the resulting charges, the consequent necessary measures.

16.2 The *Sub-Manager* also undertakes to agree on the revision of this deed as a result of regulatory and / or conventional changes.

SPECIFIC INSTRUCTIONS

A. DATA BREACH COMMUNICATION FLOW TO THE PRIVACY GUARANTOR

The flow begins with the identification of a possible compromise of personal data under the management of a security incident and concludes with sending to the Supervisor, by the *holder*, of the completed form provided by the EU Regulation 2016/679.

This flow therefore provides for the interaction and exchange of specific information with the *Data Controller* impacted by the event, in order to allow him to comply with the provisions of Articles. 33 and 34 of the *Regulation*.

Pursuant to Article 4 of the *Regulation,* "breach of personal data" (data breach) means the breach of security that accidentally or illegally involves the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

FLOW DESCRIPTION

The flow of communication to the *Guarantor* by the *Data Controller* includes the following steps:

1 If the *Sub-Manager* or *Sogei* detects a possible "personal data breach", the latter will promptly notify the *Owner* (competent IT security structure or equivalent structure thereof) that the management of a data breach is in progress , communicating a description of the incident based on the information available and assigning it a unique identifier. The *Sub-Processor* is always required to inform *Sogei* in advance of the communications he intends to send to the *Data Controller.*

2 In the event that the *Data Controller* detects the possibility of a data breach, it communicates a description of the incident to *Sogei* based on the information available, assigning it a unique identifier. If it deems it necessary, *Sogei* will notify the *Sub-Processor.*

3 The *Sub-Processor* and / or *Sogei*, coordinating the operating structures involved, collect all the evidence necessary for the *Data Controller* to verify the actual loss or disclosure of *Personal Data* and assess the extent of any violation, providing the technical details and any additional information about the incident and the progress of the activity.

4 In the event that no elements have been found that indicate the compromise of *Personal Data,* the *Sub-Processor* and / or *Sogei* terminate the data breach communication flow, notifying the *Data Controller* involved the identification of the closed incident and the related reasons.

5 In the event of a positive response (verification of evidence relating to the compromise of *Personal Data*), the *Sub-Processor* or *Sogei* formally transmit to the *Data Controller* involved, without undue delay, all the evidence collected and the information provided for in art. 33, par. 3 of the *Regulation* as far as it is concerned, in accordance with the form made available by the Privacy Guarantor.

6 The *Data Controller,* having received the communication and the relative completed form, evaluates the level of severity of the violation, according to the significance of the impact on the *Personal Data* of its ownership, and completes the notification form with the information of its competence. . The completed form must be sent to the Privacy Guarantor in the manner made available by the same within 72 hours of knowledge of the compromise of the *Personal Data* , at the same time *informing Sogei* and the *Sub-Processor.*

7 Any requests for further information or changes to the aforementioned communication necessary during the resolution activities of the event will be agreed between *Sogei* , the *Sub-Processor* and the *Data Controller.*

8 All communications between the *Data Controller*, *Sogei* and the *Sub-Processor* regarding IT security incidents are sent for information, where present, to the CERT of *Sogei* and the *Data Controller.*

9 The *Sub-Processor* must maintain accurate documentation of all recorded “personal data breaches”, including the circumstances relating to them, their consequences and the measures taken to remedy them. This documentation will be integrated with any actions taken by the *Data Controller* and appropriately communicated to the same.

INFORMATION GATHERING

The information required by the *Regulations* will be collected and reported in the data breach notification form made available to the Privacy Guarantor.

The *Sub-Manager* will enter the following information in the form, which will be communicated to the *Data Controller*:

- ✓ description of *the personal data breach;*
- ✓ time interval of the accident;
- ✓ place of the accident;
- ✓ mode of exposure to risk (type of violation, device subject to violation);
- ✓ description of the processing or storage systems involved;
- ✓ categories of interested parties;
- ✓ number of people affected by *the Data Breach;*
- ✓ type of data involved in the violation;
- ✓ technical and organizational measures applied to the data affected by the violation;
- ✓ measures activated for containment and prevention;
- ✓ possible consequence of the violation;

- ✓ proposal of the content of the communication to the contractors or to the persons concerned.

In addition to validating and possibly integrating the information provided by the *Sub-Processor*, the *Data Controller* will enter the following information in the form:

- ✓ the organizational reference data and the relative contact details of the office of the *Data Controller* affected by the data breach, who maintains relations with the Privacy Guarantor;
- ✓ the level of severity of the violation;
- ✓ any communication to interested users and the relative methods;
- ✓ if the notification to the Privacy Guarantor is not made within 72 hours, the reasons for the delay.

B. FLOW OF NOTIFICATION OF DATA BREACH TO THE OWNER BY THE INFORMATION SYSTEMS MANAGER

FLOW DESCRIPTION

The notification flow to the *Data Controller* includes the following steps:

1 As *Sub-Processor*, the DPO of the Information Systems Manager, in the course of the management of a security incident, detects a possible "breach of personal data" (Data Breach).

2 The Information Systems Operator's DPO notifies *Sogei's* CERT and its DPO that the assessment of a security incident is in progress, communicating a first summary description of the incident and assigning it a unique identifier.

3 The DPO of the Information Systems Manager verifies any and effective "violation of personal data".

4 In the event of a negative outcome of the assessment, the DPO of the Information Systems Manager ends the process, notifying the *Sogei* CERT and the DPO of the same the identification of the closed incident and the related reasons.

5 In the event of a positive outcome of the verification (ie the "violation of personal data" has been ascertained, the relative impact assessment has been carried out and the seriousness of the risk for the rights and freedoms of individuals established according to the model eventually shared) , the DPO of the Information Systems Operator communicates this immediately and without undue delay to the DDE of the Contract and to the DPO Sogei. Sogei will communicate the Data Breach to the *owner.*

Any requests for further information or changes to the aforementioned notification to the Control Authority and necessary during the resolution activities of the event will be agreed with the Information Systems Operator.

The DPO of the Information Systems Operator will keep accurate documentation of all recorded "personal data violations", including the circumstances relating to them, their consequences and the measures taken to remedy them. This documentation will be integrated with any actions taken by *Sogei* and the *Data Controller*, if appropriately communicated also to the Information Systems Manager.

INFORMATION GATHERING

The information required by the *Regulations* will be collected and entered in the notification of the Data Breach according to the following scheme.

The Information Systems Operator's DPO will enter the following information in the notification, which will be communicated by *Sogei* to the *Data Controller*:

- type of accident;
- description of the impacted service and / or of the bank / databases subject to *personal data breach* ;
- time interval of the accident;
- place of the accident;
- technical security measures applied to the violated data;
- measures activated for containment and prevention;
- description of 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 in question;
- description of the probable consequence of *the personal data breach;*
- description of the *Security Measures* adopted or proposed to be adopted to remedy the violation and also, if necessary, to mitigate any possible negative effects;
- proposal to communicate a personal data breach to the interested party / s based on an analysis of the data subject to the breach (if the breach is likely to present a high risk for the rights and freedoms of individuals) and not if any of the conditions referred to in Article 34, par. 3, of the *Regulations* , which exclude the need to communicate the violation to the interested party.