PRIVACY ANNEX

CONTRACT NO. REP. _____

1. PURPOSE AND SUBJECT OF THE DOCUMENT

This document (" *Privacy Annex* "), pursuant to art. 28 of the Regulation 2016/679, intends to regulate the obligations and instructions that the *Supplier* is required to observe if the execution of the *Contract*, including any amendments and/or additions, involves the *Processing of Personal Data* on behalf of *Sogei.*

In this case, *Sogei* could play the role of independent *Data Controller* or Data *Processor* on behalf of the *Customer Administration*. Consequently, the *Supplier* is designated (i) Data *Processor*, if Sogei plays the role of *Data Controller*, or (ii) *Sub-Data Processor,* if *Sogei* plays the role of *Data Processor* on behalf of the *Customer Administration*.

This appointment is deemed to have been accepted by the *Supplier* (s) at the time this *Annex Privacy* will be sent to *Sogei* duly signed, (ii) you want, pursuant to and by effect of art. 1327 of the Civil Code, with the fulfillment of the services inherent in the *Contract* and in any case with the start of the *Treatment activities*, regardless of which of the two events occurs first.

This *Privacy Annex*, including any attachments, constitutes an integral and substantial part of the *Contract* between *Sogei* and the *Supplier*.

In the case of a temporary grouping of companies (RTI), the *Supplier*, appointed as Data Processor or Sub-Processor, as representative of the RTI, must designate the principal companies that carry out processing operations on personal data as its Sub-Processors of the treatment.

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 case in which such *Processing* will be carried out by the *Supplier* as independent *Data Controller* or under joint ownership with *Sogei* pursuant to art. 26 of the Regulation, the latter case in which a suitable co-ownership agreement will be stipulated between the parties.

2. 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 found in the same from time to time:

- "*Customer Administration*": the Administrations and/or other entities or legal persons who are recipients of the services provided by *Sogei*, also through the *Contract*, and who could qualify as *Data Controllers*.
- "*Contract*": means the contract, including its attachments, entered into 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 convictions and offenses referred to in Article 10 of the Regulation), made available, transmitted, managed, controlled or otherwise processed by *Sogei* in its capacity as *Data Controller* or Data *Processor* on behalf of *the Client Administrations*.
- *"Director of Execution (DDE)":* subject to whom responsibility for the execution phase and the entire technical-administrative process of managing the contract is assigned;
- *"Essential elements of the treatment"*: the elements referred to in art. 28, paragraph 3, first paragraph of the Regulation.

- "*Supplier*": the contractor who, by virtue of this *Privacy Annex*, is designated by *Sogei* as Data *Processor* or *Sub-processor.*
- "*Security Incident*": the security breach involving the loss, modification, unauthorized disclosure or access to confidential data and/or information, the violation and/or malfunction *of Security Measures*, electronic tools, hardware or software to protect data and information.
- "*Security Measures*": the security measures of a physical, logical, technical and organizational nature aimed at guaranteeing a level of security adequate to the risk, including those possibly specified in *the Contract* and/or in the further documentation of contractual relevance.
- " *Personal Data Protection Rules* ": the laws, regulations, and, in general, national and European rules, including soft law, applicable in relation to the processing and/or protection and security of Personal Data, as well as as amended from time to time, including, by way of example but not limited to, Regulation (EU) 2016/679 ("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 and EU Supervisory Authorities.
- "*Persons authorized to process data*": persons who, as employees, collaborators, directors or consultants of the *Supplier,* have been authorized to process *personal data* and operate under the direct authority of the *Manager* or *Sub-manager* or *independent Data Controller*.
- *"Data processor*" or "*Manager*": the natural or legal person, public authority, service or other body that processes personal data on behalf of the *Data Controller*.
- "*Data Protection Officer (DPO)*": the subject designated by the Data Controller pursuant to art. 37 et seq. of the Regulation also called Data Protection Officer (DPO).
- "*Sole person in charge of the procedure*": the Execution Manager is the person appointed with a specific deed who carries out, in coordination with the DDE, the control and supervision activities on the execution of the contract in compliance with the company directives and according to the provisions of the contract itself. The Execution Manager, in the absence of the express appointment of the DDE, carries out the tasks and activities assigned to the latter.
- "*Sogei*": SOGEI – Società Generale d'Informatica SpA as *Data Controller* or Data *Processor*.
- "*Sub-Processor*": the natural or legal person or other public or private body which processes personal data pursuant to a written agreement with another Data *Processor*. *Sub-Data Processor* may indicate the *Supplier* when *Sogei* acts as Data *Processor* on behalf of the *Customer Administration* , or the subject to whom the *Supplier* , authorized by *Sogei* , has delegated the execution of specific *Processing activities*.
- "*Data Controller*" or "*Owner*": the natural or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of processing personal data, i.e. *Sogei* or the *Customer Administration*; when the purposes and means of such processing are determined by European Union or Member State law, the *Data Controller* or the specific criteria applicable to his designation may be established by Union or Member State law.
- "*Processing*": any operation or set of operations performed with or without the aid of automated processes and applied to *Personal Data* or set of *Personal Data* , such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form made available, comparison or interconnection, limitation, alignment or combination, cancellation or destruction.
- "*Data breach*": the breach of security which involves the accidental or unlawful destruction, loss, modification, unauthorized disclosure or access to *Personal Data* transmitted, stored or otherwise processed.

3. OBLIGATIONS AND INSTRUCTIONS FOR THE SUPPLIER

The *Supplier*, in its capacity as *Data Processor* or *Sub-processor*, undertakes to process the *Personal Data* exclusively in compliance with the instructions set out in *the Contract* and in this *Privacy Annex* and with the further instructions that may possibly be given by *Sogei* , in compliance with the obligations set forth therein and with *the Personal Data Protection Regulations*.

The provisions set out below refer to the obligations undertaken by the Supplier and the instructions that the latter undertakes to respect in relation to the *Processing of Personal Data* connected with the execution of the *Contract*. The provisions of this *Privacy Annex* can be supplemented and waived only on the basis of further and specific instructions and/or appointments by *Sogei*.

If the Supplier detects its impossibility to comply with the conditions and instructions contained in this *Privacy Annex*, even due to unforeseeable circumstances or force majeure, it will have to implement all possible and reasonable measures to guarantee the security of the *Treatments* and immediately notify *Sogei*, agreeing with this last eventual actions and/or the adoption of further *Security Measures*.

I. GENERAL OBLIGATIONS

1. The *Supplier* is authorized to process only the *Personal Data* necessary for the execution of the activities covered by the *Contract* and to the extent necessary for this purpose.

2. To this end, the *Supplier* undertakes to:

- not determine or favor through actions and/or omissions, directly or indirectly, the violation by *Sogei* and/or the *Customer Administration* (in the event that the latter is the *Data Controller*) of the *Rules on the Protection of Personal Data* ;
- promptly inform *Sogei* if it becomes aware that such *Personal Data* is inaccurate and obsolete;
- adopt, update and implement appropriate *security* measures to guarantee an adequate level of security, including confidentiality, in order to minimize the risk *of security incidents* and/or *personal data breaches* .

3. The *Supplier* also undertakes to:

a) immediately inform *Sogei* if it believes that the instructions given to it with this *Privacy Annex* and/or through further documents are, or may be, contrary to *the Personal Data Protection Regulations*;

b) guarantee the confidentiality of the *Personal Data* processed for the execution of the activities of the *Contract*;

c) not to disseminate and not communicate the *Personal Data* being *processed* , without written authorization from *Sogei* and/or the *Customer Administration* (where the latter is the *Data Controller*), without prejudice to the particular confidentiality requirements expressly specified by the Judicial Authority;

d) before starting the *Processing operations*, designate in writing and adequately instruct the *Persons authorized to process* them, also for homogeneous sectors or categories, identifying the permitted areas of operation and guaranteeing access only to the *Personal Data* strictly necessary for the execution of the *Contract*. The *Supplier* guarantees that the *Persons authorized to process* are in possession of the requisites of morality, experience, ability and reliability sufficient to ensure that the *Processing is carried out* in compliance with *the Personal Data Protection Regulations*;

e) ensure that the *Persons authorized* to process personal data under the *Contract* and this *Privacy Annex* receive adequate instructions regarding the methods of processing, in

compliance with *the Data Protection Regulations* . The *Supplier* must also guarantee that these subjects: ***(i)*** only have access to the *Personal Data* necessary to carry out the activities entrusted to them; ***(ii)*** they are committed to confidentiality or have an adequate legal obligation of confidentiality, including for the period following the termination of the *Processing* ; ***(iii)*** have received, and are receiving, the necessary training on the protection of *Personal Data from the Supplier;*

f) adopt and/or use a suitable system of identification, authentication and access authorization to *Personal Data* for *Persons authorized to Process*;

g) identify and appoint, if the conditions are met, as " *System Administrators* " ("*AdS*") 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 expedients prescribed to the holders of treatments carried out with electronic instruments in relation to the attributions of the functions of system administrator* ") and subsequent modifications and additions. In this case, the *Supplier* must prepare and keep updated a list of such subjects and, where applicable, in consideration of the methods of carrying out the services covered by the *Contract* , monitor their related activities in accordance with what is indicated in the provision last mentioned;

h) where requested by *Sogei* , possibly also upon instruction from the *Customer Administration* (where the latter is the *Data Controller*), provide the information to the interested parties, on the basis of a model agreed with *Sogei* or provided directly by the latter;

i) where necessary and applicable, support *Sogei* and/or the *Customer Administration* (in the event that the latter is the *Data Controller*) in the management of the mechanisms and/or systems for the acquisition and registration of the consents of the interested parties;

j) provide, upon request, any copy of the *Personal Data* of the employees, directors, consultants, collaborators or other personnel of the *Supplier* authorized to process, during the activities covered by the *Contract* exclusively for purposes related to the execution of the contractual and administrative-accounting activities, in addition and for the security of the offices and systems. Therefore, the *Supplier authorizes Sogei* to extract such *Personal Data* from its information systems exclusively for the aforementioned purposes and guarantees that it has correctly fulfilled, pursuant to art. 13 of the Regulation, to the obligation to inform their employees, collaborators, directors or other personnel that their personal data, in compliance with the principle of pertinence, will be communicated to third parties, and in the case that is relevant here to *Sogei* , for the exercise of the activities of the *Contract* or for the proper exercise of its activities.

4. The *Supplier* , using the conditions set out in art. 37 of the Regulation, undertakes to designate the professional figure of *the Data Protection Officer (RPD)* and to promptly communicate their contact details to *Sogei* .

I.A) *Essential elements of the treatment*

1. The *essential elements of the treatment* referred to in art. 28, paragraph 3, first paragraph, of the Regulation will be shared with the *Supplier* , through the *DDE* , during the execution of the *Contract* and, in any case, before the start of the Processing activities.

2. The *essential elements of treatment* initially communicated may be subject to integration, variation or modification with a suitable communication to be sent by *Sogei* with the same methods indicated above.

3. However, it is understood that the instructions provided with this *Privacy Annex* are valid for each *Processing* of each category of *Personal Data* referring to each category of Data Subjects and, therefore, suitable for allowing the *Supplier* to carry out the delegated *Processing in execution of the Contract*.

I.B) ***Requests and Rights of the interested parties***

1. If the *Supplier* receives complaints and/or the *Data Subjects* exercise their rights by sending the relative request directly to the *Supplier*, the latter must forward it promptly, and in any case no later than 3 days from receipt, to *Sogei* via the certified email address *dpo@pec.sogei.it*.

2. The *Supplier* will be required to check the requests of the Data Subjects only if it has been authorized by *Sogei* and/or by the *Customer Administration* (in the event that the latter is the *Data Controller*).

3. Where required, the *Supplier* lends its support and collaboration in giving written feedback, even of mere refusal, to the requests of the interested parties and to the requests of the same for the exercise of the rights provided for by the articles 15-22 of the Regulation, following the instructions received from *Sogei* and/or from the *Customer Administration* (in the event that the latter is the *Owner of the treatment*).

4. In any case, the *Supplier* must provide all the necessary support so that the reply to the interested parties takes place without unjustified delay and in any case no later than the useful and/or legal term established for replying to the requests/requests received.

I.C) ***Sub-processors***

1. The *Supplier* may resort to *Sub-Processors* for the execution of specific *Treatments*. Before the start of the *Processing activities* , the *Supplier* communicates to *Sogei* , in the figure of the *DDE* , the names and company name of the *Sub-Processors* it intends to use, as well as the *Processing activities to* be delegated, thus giving *Sogei the opportunity to* oppose the identified *Sub-Processors* . The *Supplier* also undertakes to promptly notify *Sogei* , in the figure of the *DDE* , any additions or replacements of the *Sub-Managers,* in order to allow *Sogei* to oppose such additions or replacements.

2. In the event that the *Supplier* has designated a *Sub-Manager of the treatment* , the *Supplier* and the *Sub-Manager* must, in compliance with the provisions of art. 28, par. 4 of the Regulations, be bound by a written agreement containing all the obligations and instructions regarding data protection provided for in *the Contract* and in this *Privacy Annex* , as well as any further and eventual documented instructions given by *Sogei* . Where required, the *Supplier* undertakes to transmit the act of designation of the *Sub-Processors* and any subsequent amendments. The *Supplier* , to the extent necessary to protect business secrets or other confidential information, including *Personal Data* , may remove information from the aforementioned designation deed before transmitting a copy.

3. The instructions given by the *Supplier* to the *Sub-Processors of the treatment* must in any case have the same content and pursue the same objectives as the instructions provided by *Sogei*, with reference to the treatments carried out by the *Sub-Processor*. In particular, the *Supplier* guarantees that the *Sub-Processor* ensures the adoption of all *Security Measures* in compliance with the provisions of the *Contract*, in this *Privacy Annex* and in *the Personal Data Protection Regulations* and any further instructions imparted by *Sogei*.

4. The *Supplier* undertakes to notify *Sogei* if the *Sub-Processor* fails to fulfill his obligations or the instructions received and/or implements, through actions and/or omissions, *Security Incidents* and/or violations of the *Rules on Protection of Personal Data*, it being understood that the *Supplier*

will be fully liable to *Sogei*, being unable in any way to object that said breach is due, in whole or in part, to the *Sub-Processor*.

The *Supplier* agrees with the *Sub-manager of treatment* a clause of the third beneficiary according to which, if the *Supplier* itself has de facto disappeared, has legally ceased to exist or has become insolvent, *Sogei* has the right to replace itself in relations with the *Sub -processor Responsible*, by resolving the contract and ordering the latter to proceed with the cancellation and return of personal data.

II. PROCESSING REGISTER

1. The *Supplier* is obliged to prepare, keep, also in electronic format, and update - also with the help of his *DPO* - a register of all the *Processing* activities carried out in his capacity as *Data Processor* or *Sub-processor* (hereinafter " ***Register*** "), in accordance with the provisions of art. 30, paragraph 2, of the Regulation.

2. At the request of the Supervisory Authority, the *Supplier* will make the *Register available to the* Authority itself, at the same time informing *Sogei*.

3. The *Supplier*, where requested, undertakes to support *Sogei* in the census of the *Processing* related to the *Contract*, also in order to ensure the consistency of the respective Processing *Registers.*

III. SUPPORT, COLLABORATION AND COORDINATION OBLIGATIONS

The *Supplier* provides its assistance and collaboration in ensuring compliance with the obligations set out in articles 31, 32, 33, 34, 35 and 36 of the Regulation, as described below.

III.A) Risk analysis and impact assessment

1. The *Supplier* must implement *Security Measures* to ensure a level of security appropriate to the risk and in compliance with the obligations pursuant to art. 32 of the Regulation, taking into account the state of the art, progress and technical and technological development on the subject. To this end, the *Supplier* carries out the risk analysis taking into account, in particular, the risks deriving from the accidental or illegal destruction, loss, modification, unauthorized disclosure or access to *Personal Data*.

2. The methods by which the *Supplier* performs the analysis and identification of *the Security Measures* must comply with *the Personal Data Protection Regulations,* including the applicable *cybersecurity standards,* as well as with the sector codes of conduct and/or from the certifications, where existing and/or acquired pursuant to articles 40 - 43 of the Regulation . In particular, for the purposes of verifying the correct performance of the risk analysis activities, the fact that they are based on the principles and indications present in the ISO quality standards of the sector will be taken into consideration and in particular:

a) Standard ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment;
b) Standard ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems;
c) Standard ISO/IEC 31000:2018 Risk management -- Guidelines.

3. The Supplier undertakes to assist, upon request, *Sogei and/or the Customer Administration* (in the event that the latter is the *Data Controller*) for the purposes of a periodic evaluation of the effectiveness of the *Security Measures* adopted.

4. The Supplier undertakes to assist *Sogei* and/or the *Customer Administration* (in the event that the latter is the *Data Controller*) through *Sogei* both at a technical and organizational level in carrying out

the impact assessment on the protection of personal data ("*DPIA*"), as regulated by art. 35 of the Regulation, in all cases in which the *Processing* provides for, requires or imposes the performance and/or updating of the same. The *Supplier* will lend its assistance in the preventive consultation activity of the Supervisory Authority pursuant to art. 36 of the Regulation by providing all the information necessary for this purpose.

5. In carrying out the activities referred to in this paragraph **III.A)** and, more generally, in carrying out the contractual activities involving the *Processing of Personal Data* , the *Supplier* takes into account the principles of data protection from the design and by default (" *privacy by design* " and " *by default* ") also with the aid of the instructions received; in the event that the activities covered by the *Contract* provide for the development of software, the *Supplier* nevertheless undertakes to support *Sogei* in the application of these principles by complying with the company processes and methods adopted by *Sogei itself*

III.B) *Obligations in the event of a "data breach*"

1. The *Supplier* must provide its assistance and collaboration in the fulfillment of the articles 33 and 34 of the Regulation.

2. In particular , the *Supplier* must:

a) document the *Security Incidents* and Violations of personal data referable to the *Treatments* delegated by *Sogei*, for example by preparing a specific register, including the information referred to in art. 33 of the Regulation and undertakes, upon request, to make this documentation available to *Sogei*;

b) notify Sogei, immediately and, in any case, no later than 24 hours, of any *Personal Data Violation* once the *Supplier* , or one of its *Sub-Managers* , has become aware of it or has had elements to suspect that a Violation has occurred. This communication must be drawn up in writing and contain all the information referred to in art. 33 of the Regulation and be sent to *Sogei* via the certified e-mail address cert@pec.sogei.it, together with all the documentation necessary to allow the *Data Controller* (*Sogei* or the *Customer Administration*) to notify, possibly in a preliminary way, said Violation of the competent Supervisory Authority within the terms of the law;

c) collaborate with *Sogei* and/or with the *Customer Administration* (in the event that the latter is the *Data Controller*), also in order to allow the completion of the notification process to the Supervisory Authority, in ***(i)*** investigation activities, in order to detect all the evidence necessary to evaluate the causes, nature and effects of *the personal data breach* , as well as ***(ii)*** in the adoption of the necessary actions to mitigate any damage or consequence harmful to the rights and freedoms of the Data Subjects and ***(iii)*** in the preparation and implementation, subject to approval by *Sogei* , of a plan of measures for the timely reduction of the probability that a *Personal Data Breach* similar to the one that occurred could repeat itself in the future;

d) in any case in which *Sogei* has to provide information (including details relating to the services provided by the *Supplier*) to the *Customer Administration* (in the event that the latter is *the Data Controller*) and/or to the Supervisory Authority, the *Supplier* will support *Sogei* to the extent that the requested and/or necessary information is exclusively held by the *Supplier* and/or its *Sub-Managers* .

IV. ADDITIONAL OBLIGATIONS OF THE SUPPLIER

1. The *Supplier* undertakes to transmit all the information and documentation that *Sogei* may reasonably request during the execution of the *Contract,* to verify compliance by the *Supplier* or its *Sub-Processors with* the provisions of this *Privacy Annex* and the *Rules on the Protection of Personal Data* and the instructions received.

2. The *Supplier* guarantees that *Sogei* can carry out control and evaluation activities for it and/or its *Sub-Managers* , also through authorized third parties and with reasonable notice, including through inspections and site visits in the *Supplier 's premises or physical structures* , *Processing* activity *of the Personal Data* performed by the same *Supplier* , including the work of any *AdS* , for the purpose of verifying compliance with the *Contract* , this *Privacy Annex* and the *Personal Data Protection Regulations* and 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, including any certifications in its possession. In the case of 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 warn the *Supplier* to adopt the necessary measures within a reasonable time which will be set (taking into account the nature, scope, 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 occurred), without prejudice the remedies available under the *Contract* and/or the law.

3. The *Supplier* must immediately inform and assist *Sogei* and/or the *Customer Administration* (in the event that the latter is the *Owner of the treatment*) in the event of inspections, of any measures adopted against it or in the event of proceedings before the Authorities for the protection of personal data, national and European, and/or the Judicial Authority in relation to the *Treatments* entrusted to it and except in the case in which such communication is not prohibited by provision or by law.

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

5. If *Sogei* and/or the *Customer Administration* (where the latter is the *Data Controller*) have/need, for the performance of institutional tasks, to access the *Personal Data* being *processed* that are not available through the application services, the *Supplier* undertakes, also on behalf of its *Sub-processors*, to make such *Personal Data available* according to guidelines to be agreed upon during the execution of the *Contract* and, in any case, before the start of the *Treatment activities*.

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

1. The *Supplier* must guarantee that the *Personal Data* are processed on infrastructures - including the infrastructures responsible for business continuity and disaster recovery functions, even if outsourced - located within the EU, except for justified reasons of a regulatory or technical nature.

2. In the case of remote assistance/maintenance services the performance of which in any case implies the transfer outside the EU of data traces connected to the service itself, any *Personal Data* contained in the trace must be suitably anonymised by the *Supplier*.

3. If a transfer of *Personal Data* outside the EU is necessary for the provision of services connected to the *Contract* - also to be understood as access to data from a third country - the *Supplier* may proceed with the transfer of data to a third country or an international organization outside the EU or the

European Economic Area which are covered by an adequacy decision made by the European Commission pursuant to art. 45 Regulation or by other adequate guarantees referred to in articles 46 et seq. of the Regulation itself (e.g. use of the standard contractual clauses adopted by the European Commission pursuant to Article 46, paragraph 2, letter c) of the Regulation, use of the Binding Corporate Rules - BCR), without prejudice to the need assessed in advance between the parties to adopt any additional measures to ensure the effectiveness of these guarantees.

4. The *Supplier* transmits to *Sogei* , in the person of the *DDE* , the list of non-EU data transfers it intends to carry out on the date of signing the *Contract* - containing the indication of the subject receiving the data, the country of destination and the adequate guarantees on on which the transfer is based. Through a specific communication to the *DDE* , the *Supplier* undertakes to inform *Sogei* and the *Customer Administration* (in the event that the latter is the *Data Controller*) of the termination or intention to start new data transfers outside the EU during the duration of the *Contract.*
5. In the event that the transfer is necessary to fulfill a specific requirement under European Union or Italian law to which the *Supplier is subject* , the latter is required to inform *Sogei* of this legal obligation, prior to the *Processing* , unless that the law prohibits such information for important reasons of public interest.
6. Should there be transfers of data outside the EU in the absence of the adequate guarantees referred to above, the *Supplier* will be warned against the immediate interruption of the unauthorized data transfer, without prejudice to the remedies provided by law and/or by the *Contract*.

VI. CONTRACTOR'S OBLIGATIONS AT THE TERMINATION OF THE CONTRACT

1. The duration of the *Processing* of *Personal Data* is limited and coincides with the duration of the *Contract* and its possible extensions.
2. At the end or termination of the *Processing* for any reason, the *Supplier* undertakes, for itself and also for its *Sub-Managers* , to return to *Sogei* the data which they have come into possession of in execution of the *Contract* and, subsequently, to cancel all the existing copies from any IT support, *online* and *offline* , used for the management and conservation of the same. The cases in which the conservation of the same is necessary to fulfill legal obligations are excepted.

VII. CHANGES TO THE RULES REGARDING THE PROTECTION OF PERSONAL DATA

1. In any case, if, during the validity of the *Contract*, a modification of *the Personal Data Protection Regulations occurs* which determines the need for further fulfilments, also in terms *of Security Measures*, the *Supplier will* collaborate with *Sogei* , within the limits of its own resources and technical-organizational skills, so that the necessary corrective and/or adjustment measures are developed, adopted and implemented.