PRIVACY ANNEX

This Annex is drawn up in compliance with the provisions of art. 28 of Regulation (EU) 2016/679 and is an integral and substantial part of the Contract stipulated between the Parties.

The Supplier has declared, in the context of the public procedure, to be able to ensure appropriate and adequate guarantees in terms of specialized knowledge, reliability, resources, as well as to the adoption of adequate technical, logical and organizational measures to ensure that the processing of personal data complies with the requirements of the European Regulation and, therefore, pursuant to Article 28 of the European Regulation with the signing of the Contract and its attachments, accepts the appointment as external Responsible for data processing, as Manager primary or sub - responsible - according to the designation made by SOGEI as owner or primary manager of the owner, as indicated and described in this annex and in the technical - functional documents that will be issued by Sogei together with the assignment report.

Therefore, failure by the Primary Manager or the Sub-Manager of the processing of the provisions of this Annex to be considered a serious breach of the Contract itself.

For the purposes of this Act, the term "Supplier" identifies the Contractor designated as the Primary Manager or Sub - Responsible, based on the designation made by SOGEI as Owner or primary Manager of the Owner (the Public Administrations that use of Sogei for the realization and supply of IT services).

PREMISE

OBJECT

This Annex governs the instructions that the Supplier (including the treatment by any sub-contractor or sub-supplier) undertakes to observe in the area of the processing of personal data that it will carry out on behalf of SOGEI as Owner / Primary Manager (hereinafter "Sogei") in the performance of the activities covered by the existing Contract with Sogei, guaranteeing compliance with current legislation on data protection and security.

DEFINITIONS

- *"Personal Data":* Personal Data (as well as data belonging to the particular categories of personal data referred to in Article 9 and 10 of EU Regulation 2016/679), licensed or otherwise made available, transmitted, managed, controlled or otherwise handled by Sogei (also on behalf of Sogei's Public Administrations);
- *"Rules on the Processing of Personal Data":* all applicable laws, regulations and directives 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 (GDPR), the Italian adaptation legislation, circulars, opinions and directives of the National Control Authority, the interpretative decisions adopted by the European Data Protection Board;
- *"Contract":* means the XXXX contract entered into between Sogei and Hendyplan International relating to “Troll software addons”;
- *"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":* any information relating to an identified or identifiable natural person (interested) as defined in the Rules on the Processing of Personal Data;
- "*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;
- *"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 processing 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 Union or Member State law; or Sogei or the Customer Administration xxxxx;

- *"Primary data processor":* the natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller or the Data Controller; or Sogei or the Supplier in the case of Sogei, Data Controller;
- *"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 Data Processor; or also called the XXXX Supplier or the subcontractor or subcontractor authorized by SOGEI;
- *"Supplier":* the Contractor designated as the Primary Manager or Sub - Responsible, based on the designation made by SOGEI as Owner or Primary Manager of the Owner (the Public Administrations that make use of Sogei for the construction and 'provision of IT services);
- *"Persons authorized to process data":* persons who, as employees, collaborators, administrators or consultants of the manager and / or sub-manager, have been authorized to process personal data under the direct authority of the Primary Manager or Sub responsible;
- *"Authorized third parties":* third parties, or the natural or legal person, public authority, service or other body that is not the interested party, the data controller, the data controller, who, as employees, collaborators , administrators (including system administrators) or consultants of the Supplier have been authorized to process personal data under the direct authority of the Primary Manager or the Sub-Responsible;
- *"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;
- *"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 OF PERSONAL DATA

The Supplier will comply with all the regulations concerning the Processing of Personal Data in relation to the Processing of Personal Data including those that will be issued during the term of the Contract in order to ensure, each within the scope of its activities and specific competences, an adequate level of security of the processing, including confidentiality, so as to minimize the risk of destruction or loss, even accidental, modification, unauthorized disclosure, as well as unauthorized access, even accidental or illegal, or unauthorized processing or not in accordance with the purposes of the collection.

SUPPLIER OBLIGATIONS AND INSTRUCTIONS

I. GENERAL SUPPLIER'S OBLIGATIONS

1. The Supplier is authorized to process on behalf of SOGEI (Owner / Primary Manager) 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:

- not determine or favor, through actions and / or omissions, directly or indirectly, the violation by Sogei or the Data Controller of the Rules concerning the Processing of Personal Data;
- 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 Rules concerning the Processing of Personal Data;
- 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; violations of personal data (Data Breach)
• any violation of security measures;
• all other forms of treatment of unauthorized or illegal data.

3. The Supplier undertakes to designate the professional figure of the Data Protection Manager pursuant to art. 37 GDPR and to communicate the relevant data and contacts in a timely manner to Sogei, based on the activity performed

II. INSTRUCTIONS FOR THE SUPPLIER

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

The essential elements of the processing are contained in this document, in the contract and in its attachments, as well as in the technical and functional documents that will be issued by Sogei together with the assignment report.

In particular, the aforementioned documents will contain the regulated subject, the nature and purpose of the processing, the type of personal data processed and the categories of Data Subjects.

The duration of the processing of personal data is limited, therefore it coincides with the duration of the Contract and its possible extensions.

II.B) Obligations of the Processing Provider towards Sogei

The Processing Provider undertakes to:

1. Treat the data only for the execution of the activities referred to in the subject of the Contract.

2. Treat the data in accordance with the documented instructions given by SOGEI - which, in turn, will be instructions that are compliant and adequate, during the Contract, to the instructions given by the Data Controller (in the event that the Data Controller is a public Administration or a customer of Sogei) - with this Annex and with any additional documented instructions. If the Supplier considers that an instruction is, or may be, contrary to the Data Protection Law, including the GDPR, it must immediately inform SOGEI.

3. To process the data in accordance with the documented instructions of SOGEI referred to in the previous paragraph also in cases of transfer of data to a third country or an international organization, unless required by Union or national law to which the Supplier is subject; in the latter case, the Supplier must inform SOGEI of this legal obligation before the processing begins, unless the right prohibits such information for significant reasons of public interest.

4. Ensure that the processing of Personal Data is carried out in a lawful, correct, adequate, relevant manner and is carried out in compliance with the principles set forth in art. 5 and ss. of the GDPR.

5. Guarantee the confidentiality of personal data processed for the execution of the Contract activities.

6. Guarantee that the persons authorized to process personal data by virtue of this Contract: **i)** are committed to confidentiality or have an adequate legal obligation of confidentiality; **ii)** have received, and receive, from the Supplier the necessary training regarding the protection of personal data; **iii)** access and process personal data by observing the instructions given by SOGEI.

7. Taking into account the execution of the contractual activities of the principles of data protection from the design and protection by default (privacy by design and by default) also through the use of documented instructions given by the Data Controller.

8. The Supplier undertakes to give SOGEI any copy of the personal data of the employees, directors, consultants, collaborators or other personnel of the Supplier during the activities covered by the Contract [1] exclusively for purposes relating to the execution of the contractual and administrative accounting activities as well as for the security of offices and systems. The Supplier, by signing this contract, authorizes Sogei, exclusively for the aforementioned purposes, to extract such personal data from its information systems.

9. If required by the Rules on the Processing of Personal Data, SOGEI and the Supplier agree to sign an additional agreement, modification or update that may also be necessary to allow the transfer of such personal data if they do not fall within its jurisdiction of origin pursuant to the Rules on the Processing of Personal Data.

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

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 GDPR, namely the

[1] The Supplier shall in turn inform its employees, collaborators, administrators that their personal data, in compliance with the pertinent principle, will be communicated to third parties, and in the case that is noted here at Sogei, for the exercise of the Contract activities or for the proper exercise of its activities.

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.

3. To this end, the Supplier must adopt and update a register of all the processing activities carried out on behalf of Sogei, complete with all the information required by art. 30 of the GDPR (see following paragraph III of this Annex) and make this register available to Sogei so that the requests made by the Interested parties pursuant to articles 15-23 of the GDPR.

4. If the Interested parties exercise a right provided by the GDPR by sending the related request to the Supplier, the latter must forward it promptly, and in any case no later than 3 days from receipt, by e-mail to SOGEI.

II.D) Obligations of the Supplier that makes use of Authorized Third Parties

1. The Supplier may resort to Authorized Third Parties for the execution of specific processing activities exclusively in cases where it has received express written authorization from Sogei.

2. In the event that the Supplier, with prior written authorization from Sogei, has designated an Authorized Third Party, the Supplier and the authorized Third Party must be bound by a written agreement containing all the obligations regarding data protection referred to in this Agreement and related Annexes and referred to any additional documented instructions given by SOGEI.

3. The Supplier must formulate in writing to Sogei the request for authorization to appoint an Authorized Third Party, specifying: **i)** the processing activities to be delegated; **ii)** the name / company name and the addresses of the Third Party; **iii)** the requirements of reliability and experience - also in terms of professional, technical and organizational skills as well as with reference to the security measures - of the Third Party concerning the processing of personal data; **iv)** the content of the relevant contract between the Supplier and the authorized Third Party.

4. In particular, the Supplier must guarantee that the Authorized Third Party ensures the adoption of adequate measures, logic, technical and organizational in accordance with this contract and the relevant legislation and regulations and the instructions given by SOGEI regarding data protection personal.

5. In any case, Sogei's subsequent right to oppose the addition or replacement of the Authorized Third Party with other Third Parties remains unaffected.

6. The instructions given by the Supplier to any Third Party must have the same content and pursue the same objectives as the instructions provided to the Supplier by Sogei within the limits of the treatments authorized by the Third Party.

7. To this end, Sogei can at any time verify the guarantees and the technical and organizational measures of the Authorized Third Party, also by means of audits, assessments, inspections and inspections carried out by its own personnel or by third parties. In the event that these warranties are non-existent, SOGEI, in accordance with the contractual provisions, may terminate the contract with the Supplier. In the event that at the end of the checks, inspections, audits and assessments the security measures should prove to be inadequate with respect to the risk of the processing or, in any case, unsuitable for ensuring the application of the rules on the protection of personal data, Sogei will apply to the Supplier a penalty as contractually foreseen and will warn him to have the Authorized Third Party adopt all the most appropriate measures within a reasonable period that will be set if necessary (taking into account the nature, scope, context and purpose of the processing , of the type of data and of the category of the involved subjects involved as well as of the level of risk related to the violation of the data, to the gravity of the violation occurred and the security incidents). In the event of failure by the Authorized Third Party and / or the Supplier to comply with this warning, SOGEI may terminate the Contract and enforce the final guarantee, subject to compensation for greater damages.

III. THE SUPPLIER'S TREATMENT REGISTER

1. The Supplier is obliged to prepare, store and update - also with the help of its Data Protection Manager - 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 GDPR.

2. In particular, the Supplier Register of the processing performed on behalf of SOGEI must contain:

i) the name and contact details of the Supplier (and, where applicable, Authorized Third Parties) of the processing, of each Data Controller on whose behalf the Supplier acts, of the representative (if any) of the Supplier and of the Authorized Third Party, as well as of the Data Protection Officer (DPO);

ii) the categories of treatments carried out on behalf of each Data Controller;

iii) where applicable, transfers of personal data to a third country or an international organization, including identification of the third country or international organization and, for transfers referred to in the second paragraph of Article 49 of the GDPR, the documentation of adequate guarantees;

iv) a general description of the technical and organizational security measures put in place for a correct and safe treatment pursuant to Article 32 of the GDPR.

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

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

IV.A) Safety measures.

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 GDPR. The criteria for risk assessment must be previously shared and approved by Sogei. 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.

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 GDPR).

In assessing the adequacy of the security level, the Supplier must take special account of the risks presented by the treatment (or treatments), which derive in particular from the destruction, loss, modification, unauthorized disclosure or access, in an accidental or illegal way, or from the treatment not allowed or not in compliance with the purposes of the collection, to the personal data transmitted, stored or in any case treated.

The modalities of performance of the privacy activities by design and privacy impact assessment by the Supplier for the identification of the security measures pursuant to art. 32 of the Regulations, must comply with:

- EU Regulation n. 679/2016 relating to the protection of individuals with regard to the processing of personal data, as well as to the free movement of such data and repealing Directive 95/46 / EC (General Regulation on data protection);
- Document WP 243 - Guidelines on Data Protection Officers (DPOs) of 13 December 2016;
- Document WP 248 rev. 0.1 - Guidelines concerning the impact assessment on data protection as well as the criteria to establish whether a treatment "may present a high risk" pursuant to regulation 2016/679 of 4 October 2017;
- ISO / IEC 29134 Standard: 2017 Information technology - Security techniques - Guidelines for privacy impact assessment;
- ISO / IEC 27001: 2013 standard Information technology - Security techniques - Information security management systems;
- ISO / IEC 31000 Standard: 2018 Risk management – Guidelines.

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 present in the owner's Register;

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 functionalities that make up the ICT service;
d) classification of the ICT service in terms of privacy features (purpose, lawfulness, interested, ...), and risk assessment for the organization (confidentiality, integrity and availability);
e) assessment of the necessity and proportionality of the treatments in relation to the purposes;
f) assessment of the risks to the rights and freedoms of the data subject related to the type of data processed;
g) assessment of the risks for the rights and freedoms of the interested party relative to the type of treatment, as envisaged by the WP 248 guidelines;
h) in the event of a high risk assessment for the rights and freedoms of the interested party, identification of specific PIA safety measures and relative adequacy assessment;
i) assessment of the overall intrinsic risk for the ICT service (for the organization and for the person concerned) and identification of appropriate security measures according to the principle of privacy by design and relative adequacy assessment;
j) preparation of the document containing the risk analysis, the relative safety measures and the relative adequacy assessment to be proposed to the Owner according to the Sogei standard; transposition of the eventual observations of the Owner, DPO, Privacy Guarantor and Authority.

At the end of the risk analysis, adequate safety measures pursuant to art. 32 of the GDPR must be shared and approved by Sogei and the Owner (in the event that the Owner is a public Administration customer of Sogei).

The results of the risk analysis for identifying adequate security measures will be reported by the Supplier in a specific document containing at least the following information: identification and classification of personal data also processed in terms of confidentiality and integrity; classification of the treatment also in terms of availability; assessment of the risks for the person concerned and the treatment itself; identification of security measures as required pursuant to Article 32 of the GDPR.

The identification of personal data subject to processing must follow the privacy by default criteria set forth in art. 25 of the GDPR.

According to the art. 32, paragraph 4, GDPR the Supplier must guarantee that whoever acts under his authority and has access to Personal Data does not treat such data if not properly instructed, unless the law of the Union or of the Member States requires it.

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

The Supplier must assist and cooperate fully with SOGEI and its Data Controllers, in the fulfillment activities referred to in Articles 33 and 34 of the GDPR concerning violations of personal data, or data breach.

In particular, the Supplier must:

- prepare and update a register containing all violations of personal data both from processing performed on behalf of SOGEI, in order to facilitate the latter in the investigation activities following a data breach;
- communicate to SOGEI, promptly and in any case without undue delay, that a violation of personal data has occurred since the Supplier, or an Authorized Third Party, has known or had elements to suspect their existence. This communication must be written in writing, in accordance with the criteria set by art. 33 of the GDPR and must be transmitted together with any documentation useful to SOGEI to allow it to notify, without unjustified delay to the Owner, (in the event that the Owner is a public Administration customer of Sogei), the data breach so that the Data Controller , if necessary, can notify the competent control authority of the violation within and not later than 72 hours from when it became aware of it;
- investigate the breach of personal data by adopting all the technical and organizational measures and remedial measures necessary to eliminate or contain exposure to risk, collaborate with SOGEI in investigative activities, mitigating any damage or detrimental consequence of the rights and freedoms of the Interested Parties (mitigation measures) as well as implementing a plan of measures, subject to approval by SOGEI and / or the Data Controller, in the event that the Data

Controller is a public Administration customer of Sogei, for the timely reduction of the probability that a similar data breach personal can repeat itself;

- in the event that SOGEI must provide information (including details relating to the services provided by the Supplier) to the Owner and / or the Control Authority, the Supplier will support SOGEI to the extent that the information requested and / or necessary for the Authority of control are exclusively in the possession of the Supplier and / or its Authorized Third Parties.

IV.C) Obligations of the Supplier in assessing the impact of the risk of violations of Personal Data.

1. To carry out the impact assessment of the treatments on the protection of personal data, SOGEI may consult with its Data Protection Officer (Article 35, paragraph 2, of the GDPR).

2. The Processing Provider undertakes to assist SOGEI and the Owner (in the event that the Owner is a public Administration customer of Sogei) through SOGEI, at technical and organizational level, in carrying out the impact assessment, so as governed by art. 35 of the GDPR, in all cases in which the processing foresees or requires the preliminary impact assessment on the protection of personal data (hereinafter also "PIA") or the updating of the PIA.

3. The results of the impact assessment pursuant to art. 35 of the GDPR 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).

4. The Supplier also undertakes to assist SOGEI in the activity of preventive consultation of the Control Authority pursuant to Article 36 of the GDPR.

V. ADDITIONAL GUARANTEE OBLIGATIONS OF THE TREATMENT PROVIDER

1. The Supplier undertakes to operate by adopting all technical and organizational measures, training, information and updating activities reasonably necessary to ensure that the Personal Data are accurate, correct and updated during the entire duration of the treatment - even if the processing it consists in the mere custody or control activity of the data - performed by the Supplier, or by a Third party authorized by him, to the extent that the Supplier is able to operate in this sense.

2. The Supplier undertakes to transmit to SOGEI all the information and documentation that the latter can reasonably request during the Contract in order to verify the conformity of the Supplier (or of the Authorized Third Party as sub-contractor and sub-supplier) with the this Annex, the Rules on the Processing of Personal Data and Security Measures.

3. The Supplier guarantees to SOGEI, or to its duly authorized representatives, the possibility to carry out, with reasonable notice, control and evaluation activities, also through inspections and inspections conducted by authorized subjects and appointed by SOGEI, of data processing activities Personal executed by the same Supplier, including the work of any system administrators, for the purpose of verifying compliance with the Contract (including the respective Annexes), with the Instructions of SOGEI and the Rules on Data Processing. Supplier must make available to SOGEI, without any delay and / or omission, all the information necessary to prove its compliance with the obligations set forth in the Contract. In the event that at the outcome of the periodic checks, inspections, audits and assessments the technical, organizational and / or safety measures are inadequate with respect to the risk of the treatment or, in any case, unsuitable for ensuring the application of the Regulation, SOGEI will apply to the Supplier the penalties provided for in the Contract, distrusting him to take the necessary measures within a reasonable period that will be set if necessary (taking into account the nature, the scope of application, the context and the purposes of the processing, the type of data and the category of stakeholders involved as well as the level of risk of violation and / or the seriousness of the violation occurred). In the event of failure by the Supplier to comply with this warning, Sogei may terminate the Contract and enforce the final guarantee, subject to compensation for greater damage

4. Without prejudice to the provisions of paragraph VI below, the Supplier may not transfer Personal Data to a third country or an international organization, unless it has previously obtained written authorization from SOGEI and the Owner.

5. The Supplier undertakes to promptly notify SOGEI and the Owner in the event that the Owner is a public Administration customer of Sogei, any provision of a Control Authority, or of the Judicial Authority relating to Personal Data of Sogei except for in the event that such communication is not prohibited by the provision or by law.

6. In such circumstances, unless prohibited by law, the Supplier must*: i)* inform Sogei and / or the Owner promptly, and in any case within 24 hours of receipt of the request for the exposure; *ii)* collaborate with Sogei and / or the Owner, in the event that he intends to legally oppose this communication; *iii)* guarantee the confidential treatment of such information.

7. The Supplier acknowledges and acknowledges that, in the event of a violation of the rules on the Processing of Personal Data as well as the provisions of this Annex, in addition to the application of the clauses of termination of the contract and of the penalties in addition to the any compensation for greater damage, SOGEI will have the right to resort to precautionary, injunctive and summary measures or other equitable remedy, in order to immediately interrupt, prevent or limit the processing, use or disclosure of Personal Data.

8. The Supplier shall indemnify and hold SOGEI harmless from any loss, contestation, liability, costs incurred as well as any costs incurred (also in terms of reputational damage) even in relation to a single violation of the Personal Treatment Rules and / or the Contract (including the Annexes) deriving in any case from the conduct (active and / or omissive) of his and / or his authorized agents and / or Third parties (sub-suppliers).

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

1. SOGEI or a Data Controller (Sogei Customer) may authorize in writing the Supplier, or an Authorized Third Party, to transfer Personal Data (or part of such data) to third countries or international organizations only in cases where the country third or the international organization has been the subject of an adequacy assessment by the European Commission pursuant to art. 45 of the GDPR, or, alternatively, subject to the release of the adequacy assessment carried out by the Data Controller pursuant to art. 46 of the GDPR.

2. In the event that SOGEI or a Data Controller (Sogei Customer), in relation to the execution by the Supplier of the processing of its services and / or the fulfillment of the obligations assumed with the Contract, allows the Supplier (or a sub-supplier) the transfer of *Personal data to third countries or international organizations*, the Supplier must:

- agree (and undertake that its sub-suppliers agree) to comply with the obligations set forth in the clauses of the Contract;
- to guarantee that, prior to such transfer, Sogei or the owner and / or Supplier will enter into an agreement for data access as indicated by the European Commission;
- insert in the transfer agreement of personal data the provisions of the contractual clauses and the applicable Norms regarding the Processing of Personal Data.

VII. OBLIGATIONS OF THE CONTRACTOR OF THE TREATMENT AT THE END OF THE CONTRACT.

1. The Supplier undertakes not to keep - as well as to guarantee that the authorized Third Parties do not store - the Personal Data for a period of time beyond the limit of duration strictly necessary for the execution of the services and / or the fulfillment of the obligations of referred to in the Contract, or as required or permitted by applicable law.

2. Upon expiration of the Contract or at the end of the provision of the services relating to the Processing of Data, the Supplier shall cancel or safely return to SOGEI all Personal Data as well as cancel all existing copies thereof, except as otherwise provided by the relevant Regulations of Processing of Personal Data.

3. The Supplier must document this cancellation in writing to SOGEI.

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

In the event of any change in the Rules on the Processing of Personal Data applicable to the processing of Personal Data, which generates new requirements (including new measures of a physical, technical, organizational nature, concerning the security or processing of personal data), the Supplier will work with SOGEI, within the limits of its technical, organizational and resources, so that corrective measures to adapt to the new requirements are developed, adopted and implemented during the execution of the Contract.