ZU_PIMS_MOD_SERVIZI INFORMATICI E PRIVACY_EN

Author	Privacy Office
Approved by	Mario Brocca

Version

Version	*Author*	*DPO Consultation*	*Date*	*Revision reasons*
0.0	Privacy Office		10/05/2018	First emission
1.0	Privacy Office		14/05/2021	
2.0	Privacy Office		23/09/2021	
3.0	Privacy Office	24/07/2023	25/07/2023	Insert points: 4.7 5.11 5.12 c) 6.2

DPO OPINION
ok

DATA PROCESSOR DESIGNATION
- Data Processing Agreement -
(Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)

WHEREAS

a. between the CUSTOMER and the SUPPLIER named in the contract to which this document refers (hereinafter SUPPLIER) there is a contract for the provision of computer services and/or related services (hereinafter SERVICE and/or SERVICES), of which this is an integral part;
b. in this contract the parties agree to define
   - with the term "GDPR" the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and
   - with the term "Privacy Regulation" the provisions of the GDPR as well as all other provisions of the laws of the Union or the laws of the Member States relating to the protection of personal data and their free movement.
c. c. in the performance of the SERVICE, the owner of the processing of personal data, pursuant to and for the purposes of art. 4 co 1 n. 7 of the GDPR, is the CLIENT and it is the CLIENT who is responsible for carrying out all the acts provided for by the Privacy Law for the processing of personal data, i.e. information, the collection of consent, the adoption of all the authorization, assignment, storage and other measures to implement the security system, including the related measures.

That being stated, between the Parties

IT IS AGREED AND STIPULATED

what is reported below.

1. Designation of Data Processor

1.1. For tasks that, according to the Contract for the Service, remain entrusted to the Provider, the latter, is designated as Data Processor pursuant to art. 4 co1 n.8) and to art. 28 GDPR.

1.2. The Data Processor specifies that it is able to offer sufficient guarantees to put in place appropriate technical and organizational measures in such a way that processing meets the good practices requirements and guarantees the protection of the rights of the data subjects.

2. Nature of this regulation

2.1 The nature of this Data Processing Agreement is to define the conditions under which the Data Processor agrees to process personal data on behalf of the Data Controller in the performance of the Services and the technical measures implemented by the Data Processor are specified in the technical document named Record of processing activities.

2.2 Within the framework of their contractual relations, the parties agree to comply with current regulations applicable to personal data processing (personal data) and, in particular, the Privacy Regulation.

3. Agreement duration

This Data Processing Agreement will have the duration of the Agreement to which it refers.

4. Description of the services of the Data Processor

4.1. The Data Processor is authorized to process, on behalf of the Data Controller, personal data necessary to provide the SERVICE as provided for by the contract. For data that the Data Controller has already provided and will provide, the same guarantees to have already acquired the consent of those concerned to their treatment pursuant to art. 6 co 1 lett. a) l GDPR, except for the cases indicated in that art. 6 of treatment allowed even in the absence of consent
The Data Controller guarantees the Data Processor to legitimately dispose of all the information that it will entrust to the Data Processor, assuring also that such information does not violate in any way third parties' rights.
The Data Controller retains ownership of the information that will be communicated to the data processor for the SERVICE and expressly assumes full responsibility for the content of the related personal data and releases the data processor from any obligation and/or burden of verification and/or direct and indirect control in this regard.

4.2. The nature of the operations carried out on the data is the supply of the SERVICE and/or the SERVICES indicated in the contract, therefore the Data Controller declares to entrust the relative data processing to the Data Processor.

4.3. The purpose of the treatment, the nature and type of data processed, the categories of persons concerned are those specified in the "Record of Processing Activities".

4.4. To the extent of its competence, the Data Processor, in processing the data for the provision of the SERVICE, will carry out the processing in compliance with art. 5 GDPR concerning the "Principles applicable to the processing of personal data".

4.5. For the execution of the assignment subject of this contract, the Data Controller shall make available to the Data Processor the information necessary to perform the activities for the SERVICE, also addressed to the appropriate use of the information system.

4.6. The Data Processor, pursuant to art. 28 co 3 lett. b) GDPR, identifies and assigns in writing its authorized persons, defining punctually the scope of permitted processing. The data controller declares that he/she is aware that his/her authorized persons act under his/her authority.

4.7. In order to carry out support activities on the CLIENT's/Data Controller's tools, the latter authorizes the Data Processor to establish a permanent connection to the relevant environment, with remote assistance tools, in order to enable product maintenance even in the absence of the CLIENT's employees.

5. Obligations of the Data Processor

The Data Processor, in the performance of his duties, undertakes to fulfil and observe the following obligations.

5.1. Observance of the instructions given by the Data Controller

a) The Data Processor must only process the data for the purposes specified above and for the performance of the contractual Services;
b) The Data Processor must process the data in accordance with the provisions the Record of processing activities and the Data Controller considers the security measures provided therein to be adequate.

5.2. Guarantee confidentiality

a) The Data Processor ensures the observance of the confidentiality of personal data processed under this Data Processing Agreement;
b) The Data Processor ensures that persons authorized to process personal data have committed themselves to confidentiality or have an adequate legal obligation of confidentiality and that they receive and that they are given the necessary training on personal data processing and personal data protection.

5.3. Adoption of security measures for the processing

a) The Data Processor must proceed with the processing of personal data in the presence of the measures required under art. 32 GDPR. The security measures adopted are those declared in the "Record of Processing Activities ". The Data Controller acknowledges that in some cases the Data Processor will proceed to the processing through the tools set up and configured

by the same and therefore must take all necessary precautions only if the processing is carried out outside the control of the tool set up and configured by the Data Controller;

b) If the Data Processor has adhered to a code of conduct, or has exhibited a certification, it must operate in the presence of the security measures set forth in the code of conduct or protocols referred to in the certification. In this case, the Data Controller will accept the certification as proof that the Data Processor has adopted appropriate measures with respect to the processing performed, waiving the need to perform audit activities on the SUPPLIER's systems and procedures;

c) The Data Processor, for the cases contemplated in art. 37 of the GDPR, operates by using its own Data Protection Officer (RPT or DPO.): if designated, the references are indicated in the "Record of Processing Activities";

d) In accordance with art. 30 GDPR, the Data Processor (and, where applicable, its representative, if not covered by the cases of exemption referred to in par. 5 of that article) must keep a record of all categories of processing-related activities carried out on behalf of the Data Controller, containing what is specified in co 2 of that article;

e) The records indicated are kept in written form, also in electronic format, and will be made available to the Data Controller upon request of the same and/or published in the customer area.

5.4. Appointment of a Sub processor

a) Pursuant to art.28 co 2 GDPR, with this designation, the Data Controller provides the Data Processor with express general written authorization to identify other subjects who perform, on behalf of the Data Controller, the role of Sub-Processors. The Data Processor undertakes to communicate to the Data Controller the list of all the subjects identified as Sub-Processors. In case of changes, additions or substitutions of the Sub-Processors initially communicated, these new appointments must be communicated to the owner of the treatment that will have 15 days for any opposition. The Data Processor declares and guarantees that the Sub-Processors present sufficient guarantees to implement technical and organisational measures suitable for guaranteeing compliance with the provisions of the Privacy Regulation in force, and undertakes to contractually bind the further Sub-Processors to the respect of the same obligations regarding the protection of personal data assumed by the Data Processor towards the CUSTOMER;

b) In the event that the Sub-Processor fails to fulfil its data protection obligations, the Data Processor shall retain, with respect to the Data Controller, full responsibility for the fulfilment of the obligations of the Sub-Processor.

c) It should be noted that, in all cases where the SERVICE is not provided directly to the CUSTOMER, but in favor of the final customers of the same, the Data Processor is configured as an additional Data Processor, and will be required to process the data under the same conditions determined in this Agreement.

5.5. Data Controller assistance for the exercise of the rights of the data subjects

a) As far as possible, the Data Processor - considering the nature of the processing - shall assist the Data Controller in order to enable the Data Controller to comply with requests to exercise the data subject's rights under Chapter III GDPR.
As far as possible, the Data Processor will assist the Data Controller with appropriate technical and organizational measures;

b) Relating to the right of information of data subjects, it is the responsibility of the Data Controller to provide the information referred to in Articles 13 and 14 GDPR to the data subjects for the processing operations, at the time of data collection

5.6. Assistance to the Data Controller in ensuring compliance with the obligations set out in arts. 32 to 36 of the GDPR

a) The Data Processor, considering the nature of the processing and the information available to it, must assist the Data Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR: Security of processing;
   - art 32: Notification of a personal data breach to the supervisory authority;
   - art 33: Communication of a personal data breach to the data subject;
   - art 34: Data protection impact assessment;
   - art 35: Prior consultation.

b) Assistance for Security of processing- The Data Processor has the obligation to assist the Data Controller in the implementation of security of processing, in accordance with Article 32 GDPR;

c) Special security measures of the Data Processor already in place - The Data Controller acknowledges that, for the SERVICE, the Data Processor has adequate security measures in place in compliance with the GDPR.
System Administrators. In relation to the activities carried out by the Data Processor referring to the storage of personal data and system activities directed to the maintenance of the network and the updating of the related databases and operating systems, the operators of the Data Processor will have the function of System Administrators.
The fulfilments foreseen by the Privacy Guarantor in the provision of November 27, 2008 will be managed by the Data Processor; in particular, the Data Processor will assess the subjective characteristics of the system administrators, make the individual designations, verify the activities carried out by them and record the relative accesses. In relation to the provisions of the measure itself, the Data Processor is obliged to communicate to the Data Controller the updated list of the System Administrators; the communication of such data may be in electronic or paper format and the Data Controller considers this fulfilment fulfilled also by simply making available the updated list of the names of the System Administrators in a dedicated internet area.

5.7. Assistance to the Data Controller in ensuring compliance with the obligation to notify the supervisory authority of a data breach

a) The Data Processor is obliged to assist the Data Controller in fulfilling its obligations to notify the supervisory authority of a data breach, in accordance with art. 33 GDPR. The Data Processor shall notify the Data Controller of any personal data breach within a maximum of 24 hours after becoming aware of it. This notification is accompanied by what is expressly indicated in co 3 of art. 33, useful to allow the Data Controller, if necessary, to notify this breach to the competent supervisory authority.

5.8. Assistance to the Data Controller in ensuring compliance with the obligation to notify the data subject of a data breach

a) The Data Processor has the obligation to assist the Data Controller in fulfilling its obligations to communicate a personal data breach to the data subject, in accordance with art. 34 GDPR; however, such communication must always be made by the Data Controller.

5.9. Data Processor's assistance to the Data Controller for the compliance with the obligation of the "Data protection impact assessment"

a) The Data Processor will assist the Data Controller in fulfilling the obligations of the Data Protection Impact Assessment, in accordance with Article 35 GDPR, by providing any useful information in its possession through the ""Record of Processing Activities".

5.10. Data Processor's assistance to the Data Controller in the fulfillment of the obligation related to "Prior-consultation"

a) The Data Processor shall assist the Data Controller in the prior consultation with the supervisory authority, as provided for in Article 36 of the GDPR, by providing the Data Controller with any useful information in its possession through the "Record of Processing Activities".

5.11. Data Processor's assistance in case of inspections/requests by the competent authority.

a) The Data Processor shall assist and cooperate with The Data Controller in case of inspections/requests by public authorities that may in any way affect the Data Controller.
In case of inspections to the Data Processor that concern The Data Controller, immediate notification will be given to the Data Controller, if this is possible in relation to the prerequisites of the judicial investigation carried out.

5.12. Return of all personal data at the end of the contract

a) At the end of the contract the data in the possession of the Data Processor shall be returned to the Data Controller, at the request of the same, through the delivery of the backup of the data base or files on which the personal data reside; and/or deleted within the terms defined in the "Record of Processing Activities".

Any additional copies of the backup data may be kept for the additional period indicated in the "Register of the treatment of the service" for security purposes only and not intended for communication and dissemination;

b) Notwithstanding the preceding points, the Data Processor shall retain the data in cases where the law of the Union or of the Member States provides for their retention, within the time limits imposed by such legislation or measures.

c) If the Data Controller enters into the system data from other Data Controllers who are not signatories to the contract, the Data Processor will have no responsibility with respect to such data and the deletion and backup procedures will be unique and the only ones provided for the signatory Data Controller. Any exceptions will have to be agreed and managed by design in order to determine their economic efforts.

5.13. Providing the Data Controller all information necessary to demonstrate compliance with the obligations

a) The Data Processor will make available to the Data Controller all information necessary to demonstrate compliance with the obligations set forth in art. 28 GDPR and must allow and contribute to audit activities, including inspections, carried out by the Data Controller or another entity engaged by the Data Controller - in the terms and manner better defined in art. 8 below - or by the authorities.

5.14. Case in which an instruction to the Data Processor is held in violation of the Privacy Regulation

a) If, in the Data Processor's opinion, a statement of Data Controller violates the GDPR or other provisions on data protection, the Data Controller must be immediately informed.

5.15. Observance of the principles of "privacy by design" and "privacy by default"

a) In carrying out the assignment, the Data Processor must operate in compliance with the data protection principles starting from when they are designed (privacy by design) and by default. The identification of the basic requirements of the systems and compliance with these principles will be defined on a project basis during the start-up phase of the service.

6. Obligations of the Data Controller

6.1. The Data Controller must:

- provide the Data Processor with the data required by art. 4 above;
- document all instructions regarding data processing of data by the Data Processor in writing;
- monitor, in advance and during the duration of all processing, compliance with the obligations set the Privacy Regulation by the Data Processor;
- supervise processing, carrying out audits and inspections.

6.2. If the system is used by more than one company, the Data Controller signatory to the contract will be responsible to lawfully process the data of all Data Controllers and the SUPPLIER will manage the system and ancillary activities related to the contract with respect only to the signatory Data Controller.

7. Places where data are and will be stored

7.1. The data will be processed by the Data Processor in the places indicated in the "Record of Processing Activities". If in the future, processing needs to be carried out in non-EU countries, the Data Processor shall immediately inform the Data Controller to agree on guarantees that it will take according to the place where the processing will be carried out;

7.2. If the Data Processor will be required to make a transfer of data to a third country or international organization, by virtue of the laws of the Union or the laws of the member state to which it is subject, it must inform the Data Controller about this legal obligation before the transfer in order to obtain authorization, unless the law prohibits such information for important reasons of public interest.

8. Controls

8.1. The Data Controller, also through periodic checks, reserves the right to monitor the timely observance of legal provisions on data processing and compliance with the instructions indicated in this document. The Data Processor shall allow the Data Controller, providing full cooperation, to conduct periodic audits on the adequacy of security measures and observance of Privacy Regulation and provisions of the Data Controller itself;

8.2. Each audit activity requested by the Data Controller shall be notified within at least 10 Business Days advance written notice to the Data Processor. For the purpose of this article “Business Days” means form Monday to Friday excluding bank holidays in the country where the Data Processor has its registered office.
It is further agreed by the parties that in the event activities requested involve charges and expenses not provided for in this contract, all requests from the Data Controller must be managed at project level with an estimate of the costs necessary for their implementation (whether these are penetration tests, vulnerability assessments, etc.)