

Contractual act between the Data Controller and the Data Processor pursuant to Article 28 of European Regulation 679/2016, with appointment as system administrator pursuant to the Provision of the Data Protection Authority of 27/11/2008, as subsequently amended and supplemented.

[CONTROLLER] (hereinafter the Data Controller or Controller), pursuant to and for the purposes of Regulation (EU) 2016/679, by means of this act

**GOVERNS, PURSUANT TO ARTICLE 28 OF REGULATION (EU) 2016/679,
THE RELATIONSHIP WITH THE DATA PROCESSOR
WITH SYSTEM ADMINISTRATION FUNCTIONS**

the company COMPET-E srl in relation to the following processing operation(s):

SCOPE	ASSIGNED ACTIVITIES AND TASKS	ASSIGNED SYSTEMS	CONTRACTUAL RELATIONSHIP
System administrator	System administrator - GRC CORA software	GRC CORA	Protocol no. aaaa/0000
System administrator	System administrator - WiseMap software	WiseMap	Protocol no. aaaa/0000

SECTION I

Clause 1

Purpose and scope

- The purpose of this contractual act is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation), and with the Provision of the Italian Data Protection Authority 'Measures and precautions prescribed to controllers processing personal data with electronic tools with regard to the assignment of system administrator functions' of 27 November 2008 (Official Gazette no. 300 of 24 December 2008), as amended and supplemented on 25 June 2009. A System Administrator is defined as the professional figure responsible for the management and maintenance of processing systems used to process personal data, including database management systems (database administrator), complex software systems such as ERP (Enterprise resource planning) systems used in large companies and organisations, local networks and security equipment, and the hardware and software systems that enable the use of the corporate network, internet and e-mail service (network administrator), insofar as they allow intervention on personal data.
- For this purpose, the standard contractual clauses between controllers and processors (hereinafter the 'clauses'), established by the Commission in Implementing Decision (EU) 2021/915 of 4 June 2021 pursuant to Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, are used.
- The clauses apply to the processing of personal data specified in Annex I.

- d) Annexes I to III form an integral part of this act.
- e) The clauses are without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- f) The clauses do not, in themselves, ensure compliance with the obligations relating to international transfers pursuant to Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

Clause 2

Invariability of the clauses

- a) The parties undertake not to modify the clauses except to add or update information in the annexes.
- b) This does not prevent the parties from including the standard contractual clauses set out in these clauses in a broader contract, or from adding other clauses or additional safeguards, provided that they do not directly or indirectly contradict these clauses or prejudice the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- a) Where these clauses use terms defined, respectively, in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, those terms shall have the same meaning as in the relevant Regulation.
- b) These clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, respectively. c) These clauses shall not be interpreted in a way that is not consistent with the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725, or that prejudices the fundamental rights or freedoms of data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these clauses and the provisions of related agreements in force between the parties at the time of acceptance of these clauses, or concluded subsequently, these clauses shall prevail.

Clause 5

No additional remuneration

No additional remuneration shall be due to the Processor or to the System Administrators for the performance of the activities referred to in this act. Accordingly, the remuneration indicated in the main contract shall remain fixed and unchanged and shall include the obligations arising from this appointment as Data Processor.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of the processing

The details of the processing operations, in particular the categories of personal data and the purposes of the processing for which the personal data are processed on behalf of the controller, are specified in Annex I.

Clause 7

Obligations of the parties

7.1. Instructions

- a) The processor shall process the personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The controller may also give subsequent instructions throughout the duration of the processing of personal data. Such instructions shall always be documented.
- b) The processor shall immediately inform the controller if, in its opinion, the controller's instructions infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or applicable Union or Member State data protection provisions.
- c) The Processor shall fully comply with the Provision of the Italian Data Protection Authority of 27 November 2008 (published in Official Gazette no. 300 of 24/12/2008), as amended and supplemented by the provision of 25 June 2009 (published in Official Gazette no. 149 of 30/06/2009), concerning the appointment of System Administrators and, therefore, shall:
 1. Identify the natural persons appointed as system administrators after assessing their experience, skills and reliability; such persons must provide adequate guarantees of full compliance with the provisions in force on processing, including the security profile;
 2. In the appointment of such natural persons, analytically list the permitted areas of operation according to the assigned authorisation profile;
 3. Communicate to the Controller the identifying details of the natural persons appointed as system administrators.
 4. Allow the Controller to verify its work as system administrator at least annually, in order to check its compliance with the organisational, technical and security measures relating to personal data processing provided for by the applicable rules.
 5. Adopt suitable systems for recording logical access (IT authentication) to processing systems and electronic archives by system administrators. The records (access logs) must have characteristics of completeness, immutability and verifiability of their integrity that are adequate for the verification purpose for which they are required. The records must include time references and a description of the event that generated them, and must be retained for an appropriate period, not shorter than six months.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purposes of the processing set out in Annex I, unless further instructions are given by the controller.

7.3. Duration of the personal data processing

The processor shall process the personal data only for the duration specified in Annex I.

7.4. Security of processing

- a) The processor shall implement at least the technical and organisational measures specified in Annex II to ensure the security of the personal data. This includes protection against any security breach leading to accidental or unlawful destruction, loss,

alteration, unauthorised disclosure of, or access to, the data (personal data breach). In assessing the appropriate level of security, the parties shall duly take into account the state of the art, implementation costs, and the nature, scope, context and purposes of processing, as well as the risks for data subjects.

- b) The processor shall grant access to the personal data being processed to members of its personnel only to the extent strictly necessary for the performance, management and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

Where the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ('sensitive data'), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

- a) The parties shall be able to demonstrate compliance with these clauses.
- b) The processor shall respond promptly and adequately to requests for information from the controller relating to the processing of data in accordance with these clauses.
- c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in these clauses and deriving directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall allow for and contribute to audits of the processing activities covered by these clauses, at reasonable intervals or where there are indications of non-compliance. In deciding on a review or audit, the controller may take into account relevant certifications held by the processor.
- d) The controller may choose to conduct the audit itself or to appoint an independent auditor. Audits may also include inspections at the processor's premises or physical facilities and, where appropriate, shall be carried out with reasonable notice.
- e) Upon request, the parties shall make the information referred to in this clause, including the results of any audits, available to the competent supervisory authority or authorities.

7.7. Use of sub-processors

- a) Pursuant to Article 28(2) of Regulation (EU) 2016/679 and Article 29(2) of Regulation (EU) 2018/1725, the controller authorises the processor to engage the sub-processors listed in Annex III. The Processor shall keep that annex updated and shall inform the controller of any intended changes concerning the addition or replacement of other processors: where the controller, once informed, does not object to such changes within 15 days of that information, those changes shall be deemed authorised by the controller.
- b) Where the processor engages a sub-processor to carry out specific processing activities (on behalf of the processor), it shall enter into a contract imposing on the sub-processor, in substance, the same data protection obligations as those imposed on the processor in accordance with these clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject under these clauses and Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) At the controller's request, the processor shall provide the controller with a copy of the contract concluded with the sub-processor and of any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor may redact information from the contract before providing a copy.
- d) The processor shall remain fully liable to the controller for the performance of the sub-processor's obligations arising from the contract entered into by the sub-processor with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

- e) The processor shall agree with the sub-processor a third-party beneficiary clause under which, if the processor has factually disappeared, has ceased to exist in law or has become insolvent, the controller shall have the right to terminate the contract with the sub-processor and to instruct the latter to delete or return the personal data.

7.8. International transfers

- a) Any transfer of data to a third country or an international organisation by the processor shall be carried out only on documented instructions from the controller or in order to comply with a specific requirement under Union or Member State law to which the processor is subject, and in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- b) The controller agrees that, where the processor engages a sub-processor in accordance with clause 7.7 to carry out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

- b) The processor shall promptly notify the controller of any request received from a data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- c) The processor shall assist the controller in fulfilling its obligations to respond to requests from data subjects exercising their rights, taking into account the nature of the processing. In fulfilling the obligations referred to in points a) and b), the processor shall follow the controller's instructions.
- d) In addition to the obligation to assist the controller in accordance with clause 8, point b), the processor shall also assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - 1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ('data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - 2. the obligation, prior to processing, to consult the competent supervisory authority or authorities where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - 3. the obligation to ensure that personal data are accurate and up to date, by informing the controller without delay where the processor becomes aware that the personal data it is processing are inaccurate or outdated;
 - 4. the obligations under Article 32 of Regulation (EU) 2016/679.
- e) The parties shall set out in Annex II the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this clause, as well as the scope and extent of the assistance required.

Clause 9

Notification of a personal data breach

In the event of a personal data breach, the processor shall cooperate with the controller and assist it in fulfilling the obligations incumbent on the latter under Articles 33 and 34 of Regulation (EU) 2016/679 or Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of the processing and the information available to the processor.

9.1. Breach concerning data processed by the controller

In the event of a personal data breach concerning personal data processed by the controller, the processor shall assist the controller:

- a) in notifying the personal data breach to the competent supervisory authority or authorities, without undue delay after the controller has become aware of it, where applicable (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- b) in obtaining the following information which, in accordance with Article 33(3) of Regulation (EU) 2016/679, must be stated in the controller's notification and include at least:
 - 1. the nature of the personal data including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 2. the likely consequences of the personal data breach;
 - 3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all the information at the same time, the initial notification shall contain the information available at that time, and the remaining information shall be provided subsequently, as soon as it becomes available, without undue delay.

- c) in fulfilling, in accordance with Article 34 of Regulation (EU) 2016/679, the obligation to communicate the personal data breach to the data subject without undue delay, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Breach concerning data processed by the processor

In the event of a personal data breach concerning personal data processed by the processor, the processor shall notify the controller without undue delay after becoming aware of it. The notification shall contain at least:

- a) a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and data records concerned;
- b) the contact details of a contact point from which more information concerning the personal data breach can be obtained;
- c) the likely consequences of the personal data breach and the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all the information at the same time, the initial notification shall contain the information available at that time, and the remaining information shall be provided subsequently, as soon as it becomes available, without undue delay.

The parties shall set out in Annex II all other elements that the processor is required to provide when assisting the controller in fulfilling the obligations incumbent on the controller under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the clauses and termination

- a) Without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, where the processor breaches the obligations incumbent on it under these clauses, the controller may instruct the processor to suspend the

- processing of personal data until the latter complies with these clauses or until the contract is terminated. The processor shall promptly inform the controller if, for any reason, it is unable to comply with these clauses.
- b) The controller shall be entitled to terminate the contract with regard to the processing of personal data in accordance with these clauses where:
1. the processing of personal data by the processor has been suspended by the controller in accordance with point a) and compliance with these clauses is not restored within a reasonable time and in any event within one month of the suspension;
 2. the processor is in substantial or persistent breach of these clauses or of the obligations incumbent on it under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 3. the processor fails to comply with a binding decision of a competent court or of the competent supervisory authority or authorities regarding its obligations under these clauses or Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) The processor shall be entitled to terminate the contract with regard to the processing of personal data under these clauses where, after informing the controller that its instructions infringe applicable legal requirements pursuant to clause 7.1, point b), the controller insists on compliance with the instructions.
- d) After termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all personal data to the controller and delete existing copies, unless Union or Member State law requires storage of the personal data. Until the data are deleted or returned, the processor shall continue to ensure compliance with these clauses.

ANNEX I

Description of the processing

Categories of data subjects whose personal data are processed:

- Customers;
- Suppliers;
- Employees and collaborators;
- **Visitors.**

Categories of personal data processed

- Personal data (Art. 4(1) GDPR) - Personal and/or identification data

Nature of the processing

- System Administrator - GRC CORA software.
- System Administrator - Wisemap software.

Purposes for which the personal data are processed on behalf of the controller

- Customer assistance purposes;
- Purposes of defending the controller's rights in any judicial or extrajudicial disputes.

Duration of the processing

- Maximum of 12 years from the conclusion of the contractual activity.

ANNEX II

**Technical and organisational measures, including technical and organisational measures to ensure data security
(to be completed by the processor)**

Below is the list of security measures adopted within our organisation / equipment:

TECHNICAL		ORGANISATIONAL	
X	Anti-theft and alarm systems	X	Controlled access (physical access privileges)
X	Antivirus	X	Processing agreements (DPA) with other processors
X	Locked cabinets	X	Training
X	IT authentication	X	Regulations and/or usage policies
X	Authorisation (logical access privileges)	X	Appointment deeds pursuant to Art. 2-quaterdecies of the Italian Privacy Code
X	Backup	X	Processing authorisation and instruction deeds
X	Business continuity	X	Internal verification audits
X	Firewall	X	Damage insurance contracts
X	Log management		
X	Penetration test		
X	Air conditioning systems		
X	Fire prevention systems		

Specific security measures applied to SaaS services (if covered by the contract) on our clouds:

TECHNICAL		ORGANISATIONAL	
X	Anti-theft and alarm systems	X	Controlled access (physical access privileges)
X	Antivirus	X	Processing agreements (DPA) with other processors
X	Locked cabinets	X	Appointment deeds pursuant to Art. 2-quaterdecies of the Italian Privacy Code
X	IT authentication	X	Processing authorisation and instruction deeds
X	Authorisation (logical access privileges)	X	Internal verification audits
X	Backup	X	Damage insurance contracts
X	Log management	X	Training
X	Disaster recovery	X	Regulations and/or usage policies
X	Firewall	X	Security service
X	Credential change procedures		
X	Separation (logical)		
X	Air conditioning systems		
X	Fire prevention systems		
X	Video surveillance		
X	WAF (Web Application Firewall)		
X	2FA (2-Factor Authentication)		

ANNEX III

[illegible]
