

External Data Processor Appointment Agreement

onOffice Italia Srl, with its registered office in Turin – Via Vela, 29 – VAT Number 12250950016 (hereinafter referred to as “Contractor” or “Processor”), possesses the necessary technical and organizational expertise, as well as knowledge of the purposes and methods of processing personal data, the security measures to ensure the confidentiality, integrity, and availability of personal data processed, and the regulations governing the protection of personal data. This applies to the processing of personal data on behalf of the Client (“Controller”) within the scope of the services specified in the contract.

onOffice Italia Srl is appointed as the Data Processor pursuant to Article 28 of the GDPR. Furthermore, the Controller intends to grant general authorization for the appointment of additional Sub-processors.

The data subjects concerned by the processing are those whose data are managed by the Controller as part of the services provided. Depending on the activated services, the subject of data processing may include:

- a) General personal data (e.g., first name, last name, address, date and place of birth, tax code, contact information such as phone number and email address).
- b) Special categories of personal data (e.g., information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and data concerning a person’s sex life or sexual orientation).

By signing this document, the parties agree to regulate their mutual relationship regarding the processing of personal data carried out by the Processor on behalf of the Controller.

1. Appointment of the Data Processor

By signing this document, which forms an integral part of the Contract, the Controller appoints onOffice Italia Srl as the Data Processor pursuant to Article 28 of Regulation (EU) 2016/679. The Processor is responsible for carrying out the processing operations on personal data necessary to fulfill the obligations arising from this Contract. By signing this agreement, the Processor accepts all terms outlined below, confirms its full understanding of its obligations, and agrees to process personal data in accordance with the instructions provided by the Controller.

2. Nature and Duration Processing

The processing shall be carried out by the Processor as part of the existing contractual relationship with the Controller and for purposes related thereto. This appointment shall take effect upon its signing and remain in force until the termination of the Contract.

3. Rights of the Data Controller

The Controller has the right to obtain from the Processor all information regarding the organizational and security measures adopted to ensure compliance with instructions and legal obligations. Furthermore, the Controller has the right to conduct audits or specific inspections at its own cost to verify the protection and security of personal data.

4. Obligations of the Data Processor

The Data Processor undertakes to comply with Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), the Privacy Code as amended by Legislative Decree No. 101 of August 10, 2018, and any specific instructions provided by the Data Controller. Furthermore, the Data Processor shall consider the guidelines and measures issued by the Italian Supervisory Authority, the Article 29 Working Party, and the European Data Protection Board in relation to the processing activities performed.

The Data Processor agrees to:

- Process only the personal data that is necessary and/or instrumental to the execution of this Contract.
- From the date of signing this document, disclose personal data to its Sub-processors strictly to the extent necessary for fulfilling the obligations under this Contract, or as required by applicable legal obligations or European regulations.
- Cooperate with the Data Controller at all times to ensure the proper and lawful processing of personal data.
- Provide the Data Controller with any reasonably requested information or documentation to facilitate compliance with legal obligations and to verify the implementation of appropriate technical and organizational measures.
- Retain personal data only for as long as necessary and for a duration specifically indicated to the Data Controller. Upon the expiry of this period, the data shall be securely deleted.

In particular, the Data Processor agrees to adhere to the obligations and instructions detailed below.

4.1. Adequate Technical and Organizational Measures and Personal Data Breaches

The Data Processor shall implement appropriate technical and organizational measures as required by Italian and European regulations on personal data protection, as well as any provisions issued by the Supervisory Authority, the Article 29 Working Party, and the European Data Protection Board.

Taking into account advancements in technology, the nature of the personal data, the characteristics of processing activities, and the risks to individuals' rights and freedoms, the Data Processor shall adopt measures to mitigate risks such as intentional or accidental damage, data loss, unauthorized access, unauthorized processing, or processing for purposes inconsistent with this Contract.

Specifically, the Data Processor is obligated to:

- Implement all measures outlined in Article 32 of Regulation (EU) 2016/679 to ensure the confidentiality, integrity, and availability of personal data.
- Avoid transferring the Data Controller's personal data outside the usual place of work unless explicitly authorized by the relevant authorities, including regulatory or supervisory authorities.
- Maintain a record of processing activities pursuant to Article 30 of the GDPR for operations conducted on behalf of the Data Controller.
- Provide the Data Controller with the name and contact details of the designated Data Protection Officer (DPO), if applicable, in compliance with Articles 37–39 of the GDPR.

- Assist the Data Controller in ensuring compliance with obligations related to:
 - Security of processing.
 - Notification of a personal data breach to the Supervisory Authority (Article 33, GDPR).
 - Communication of a personal data breach to affected data subjects (Article 34, GDPR).
 - Conducting data protection impact assessments (Article 35, GDPR).
 - Prior consultations with Supervisory Authorities (Article 36, GDPR).

4.2. Personal Data Breaches

In the event of a personal data breach—defined as a security incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed by the Data Processor on behalf of the Data Controller—the Data Processor shall:

- Notify the Data Controller without undue delay, and no later than 24 hours after becoming aware of the breach. This notification shall include comprehensive details about the breach, such as the nature of the personal data breach, the categories and approximate number of data subjects involved, the categories and approximate number of data records affected, the consequences of the breach, and any mitigation measures taken.
- Assist the Data Controller in managing the breach and its consequences, particularly regarding communications with affected data subjects and regulatory authorities.

Propose corrective actions to the Data Controller and promptly implement any corrective measures approved by the Data Controller to mitigate risks associated with the breach. These actions shall ensure an appropriate level of security based on the risks related to the processing activities.

4.3. Privacy Documentation

The Data Processor must maintain up-to-date documentation concerning the protection of personal data, as required by Italian and European legislation. This includes developing and adhering to procedures outlining appropriate technical and organizational measures.

4.4. Requests from Data Subjects

Considering the nature of the processing activities, the Data Processor shall assist the Data Controller in responding to data subject requests to exercise their rights, in accordance with Article 12 of Regulation (EU) 2016/679. If the Data Processor receives a data subject request, it shall:

- Update the personal data of the data subject (e.g., rectify or delete data) as required.
- Where the request exceeds the Data Processor's usual responsibilities, coordinate with the Data Controller's designated functions to address the request.
 - coordinate, where necessary and within their area of responsibility, with the corporate functions designated by the Data Controller to manage relations with the data subjects;
 - assist and support the Data Controller with appropriate technical and organizational measures to fulfill the Data Controller's obligation to respond to requests for the exercise of data subjects' rights (within the scope and context of the role held and the responsibilities of the Data Processor).

4.5. Authorized Personnel for Data Processing

The Data Processor shall:

- Instruct authorized personnel on data processing activities, including the implementation of necessary security measures to prevent data destruction, loss, or unauthorized access.
- Monitor and periodically evaluate compliance with these instructions.
- Limit access to personal data to those strictly necessary for performing assigned duties.
- Regularly review and confirm the validity of access permissions granted to authorized personnel.
- Ensure that authorized personnel commit to maintaining data confidentiality and are fully trained on relevant data protection laws and best practices.
- Ensure that their employees and collaborators are capable and fully knowledgeable of the primary and secondary regulations regarding personal data protection.

5. Sub-processors and Third Parties

The Data Processor may communicate or make the Data Controller's Personal Data available to one or more Sub-processors in order to delegate specific processing activities, as outlined in this Agreement.

To ensure compliance with Regulation (EU) 2016/679 (GDPR), the Privacy Code, and the provisions of this Agreement, the Data Processor undertakes to appoint Sub-processors and ensure that they agree to terms equivalent to those governing the relationship between the Data Controller and the Data Processor. Such terms shall be formalized through legally binding agreements or contracts.

Sub-processors are permitted to process the Personal Data strictly to the extent necessary for the performance of the contract between the Data Controller and the Data Processor, and always in accordance with the terms of this Agreement. The Parties understand that Sub-processors shall also be bound by the same limitations and obligations imposed on the Data Processor.

Specifically, the Data Processor undertakes to:

- Upon the Data Controller's explicit request, disclose to the Data Controller the requirements for appointing a Sub-processor, including their technical, organizational, and knowledge-based competencies regarding the purposes and methods of processing Personal Data, as well as the security measures already implemented by the Sub-processor.
- Upon the Data Controller's explicit request, inform the Data Controller of the specific activities intended to be delegated to the Sub-processor.
- Execute a written agreement with each Sub-processor, ensuring that they comply with obligations equivalent to those imposed on the Data Processor under this Agreement, including the implementation of security measures as required under Article 32 of the GDPR. Such agreements shall provide sufficient guarantees regarding technical and organizational measures to ensure compliance with applicable data protection legislation.

If any Sub-processor or external collaborator fails to fulfill their data protection obligations, whether partially or fully, the Data Processor expressly guarantees to indemnify the Data Controller against any liabilities arising from such negligence or omissions.

The Data Processor shall not communicate, transfer, or share the Data Controller's Personal Data with Third Parties unless required by law, in which case the Data Processor will notify the Data Controller in advance.

6. Controls and Audit Activities

The Data Processor shall allow the Data Controller to verify compliance with the terms of this Agreement. If the Data Processor identifies that any instruction provided by the Data Controller contravenes applicable data protection laws, the Data Processor is obligated to immediately inform the Data Controller.

The Data Controller reserves the right to conduct audits regarding the Data Processor's handling of the Data Controller's Personal Data, subject to a notice period of at least three business days.

To this end, the Data Controller may periodically issue questionnaires to the Data Processor regarding compliance with data protection regulations and security standards, which must be duly completed and returned. Additionally, the Data Controller may, at its own expense, conduct sample checks or specific audits on Personal Data protection and security at the Data Processor's premises, using designated personnel.

The Data Processor must make all necessary information available to the Data Controller upon request to demonstrate compliance with this Agreement and to facilitate any audit activities. Such audits shall be conducted periodically or according to methods mutually agreed upon by the Parties.

7. Termination of Processing

Upon the termination of the processing activities entrusted to the Data Processor and the underlying contractual relationship, for any reason, the Data Processor shall, at the Data Controller's discretion:

- Return all Personal Data to the Data Controller and provide a written declaration confirming that no copies remain in their possession, except where legal retention obligations apply.
- Permanently delete all Personal Data from physical and electronic archives unless retention is required by law.

8. Agreement on the Transfer of Data Abroad

The Data Processor shall limit the processing and storage of Personal Data to countries within the European Union. The Data Processor is expressly prohibited from transferring Personal Data to non-EU countries that lack adequate protection or fail to comply with the safeguards required under Regulation (EU) 2016/679, such as adequacy decisions by the European Commission, Binding Corporate Rules (BCRs), or standard contractual clauses.

The Data Processor shall not transfer or process Personal Data outside the European Union without prior written authorization from the Data Controller. If such authorization is granted, the Data Processor must ensure that the transfer complies with GDPR requirements and document the implementation of adequate safeguards.

It is understood between the Parties that the Supplier is obligated to ensure that the methods of data transfer, including adherence to the standard contractual clauses approved by the European Commission and the conditions stipulated therein, maintain consistent, documented, and legally valid standards throughout the duration of this Agreement.

9. Liability for Breach of Provisions

Pursuant to Article 82(4) of the GDPR, if the Data Controller and the Data Processor are jointly responsible for processing activities that cause damage, both parties shall be jointly liable to ensure effective compensation for the affected data subject.

The Data Processor shall promptly inform the Data Controller of any circumstances that may impact its ability to fulfill its obligations under this Agreement, including changes arising from technological developments.

The Data Controller retains the right to recover from the Data Processor any compensation paid to third parties due to violations attributable to the Data Processor, pursuant to Article 82(5) of the GDPR.

In the event of a delay or failure to notify the Data Controller of a data breach, the Data Controller may claim damages equal to any penalties imposed by the Supervisory Authority, as well as additional losses resulting from compensation to data subjects or reputational harm.

Without prejudice to Articles 82, 83, and 84 of Regulation (EU) 2016/679, in the event of a breach of the provisions of this designation concerning the purposes and methods of data processing, any actions taken contrary to the instructions provided herein, or failure to fulfill the obligations specifically imposed on the Data Processor by Regulation (EU) 2016/679, the Data Processor shall be deemed a Data Controller and held directly liable for any applicable sanctions.

10. Consideration

No consideration is owed for the activities covered by this Agreement.

11. Termination

Any breach of this Agreement shall constitute grounds for immediate termination by the Data Controller. The Data Controller may also terminate this Agreement if it deems the Data Processor's guarantees insufficient for compliance with this Agreement or the GDPR.

12. Survival of Clauses

Clauses that, by their nature, are intended to survive termination of the Agreement shall remain in effect after its conclusion.

13. Communications

All communications between the Data Controller and the Data Processor under this Agreement must be conducted via email or certified electronic mail to the following address: contatti@onOffice.com.

14. Acceptance of the Appointment

This appointment, made pursuant to Article 28 of Regulation (EU) 2016/679, forms an integral part of the contract executed between the Parties. By signing this appointment, the Parties acknowledge and accept all conditions set forth in the preceding clauses. In particular, the Processor expressly accepts their appointment concerning the personal data necessary for fulfilling the obligations specified in the Agreement.

The Processor confirms their awareness of the obligations imposed by Regulation (EU) 2016/679 and the Privacy Code. Furthermore, the Processor undertakes to perform their assigned tasks in strict compliance with the provisions and responsibilities outlined in this appointment.

This appointment shall remain valid and enforceable until the termination of the Agreement, regardless of the reason for its cessation.