OSPEDALE POLICLINICO SAN MARTINO
Sistema Sanitario Regione Liguria
Istituto di Ricovero e Cura a Carattere Scientifico

Modello di Data Processing Agreement_ENG

DATA PROCESSING AGREEMENT

(art. 28 of EU Regulation 2016/679)

IRCCS Ospedale Policlinico San Martino, with registered office in Genoa, Largo Rosanna Benzi 10 - 16132,CF/P. IVA n. 02060250996,as Data Controller (hereinafter Policlinico or Controller) in the person of its Legal Representative, the General Director Dr. ___________________________________ (*insert the name of the General Director in office*),

WHEREAS

- with_________________________(*insert name of the provision: resolution, determination, other*) no. _______________ of _____________________ has been approved/authorized ____ (*insert references of the contract / agreement / other agreement or the title of the project, study, other*) stipulated with the Company ____ (*insert the name / corporate name of the Company*), with registered office in ____ (*insert address*) VAT number/Tax code ____ having as its object ____ ____ ____ (*insert a brief description of the object of the contract / agreement / other agreement or of the project, study, other*) expiring on _____________ (*insert the expiry date indicated, if applicable*);
- for the execution of the legal relationship identified above and for the completion of the consequent activities, the firm/company necessarily carries out personal data processing operations on behalf of the Policlinico;
- Article 28 of Regulation (EU) 2016/679 on the protection of personal data, hereinafter GDPR, provides that if processing is carried out on behalf of the Data Controller, the latter shall only use Data Processors who guarantee the adoption of adequate technical and organizational measures, so that the processing complies with data protection legislation and guarantees the protection of the rights of the interested party;
- the delegation of such processing activities, in accordance with the provisions of art. 28 of the GDPR, must be governed by a contract or other legal act that binds the Processor to the Controller and that stipulates the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the Controller;
- the Data Controller, by signing this legal document, guarantees to the Data Controller that he/she possesses specialist knowledge, possesses the requisites of experience, ability and reliability suitable to guarantee full compliance with the current provisions on data protection, including the profile relating to security and the protection of the rights of the interested parties;

All of the above being an integral and substantial part of this document,

APPOINTS

____

(insert the name/company name of the firm/company to be nominated)

DATA PROCESSOR

in relation to the processing activities necessary for the execution of the legal relationship reported in the introductionand described in the continuation of this document.

The Firm/Company, responsible for the processing of personal data, has the task and responsibility of fulfilling all that is necessary for compliance with the provisions in force regarding the processing of personal data and is required to comply with the following operating instructions (section II), scrupulously observing the indications given with this document as well as with subsequent amendments or additions.

The appointment of Data Processor automatically expires upon expiration or termination of the relationship established with the Data Controller. In the event that the duration of the processing exceeds the duration of the underlying relationship, the qualification of Data Processor is maintained for the entire duration of the processing, as regulated by art. 2, and no longer.

Section I

DESCRIPRION OF THE DATA PROCESSING

ART. 1 – PROCESSING ACTIVITIES

The Data Processor is hereby assigned the task of carrying out personal data processing operations in order to carry out the following activities:

____
____
____
____

(indicate only the specific activities for which the Company/Society carries out processing operations on behalf of the Policlinico, with reference to which it is appointed as Data Controller)

The processing of personal data entrusted to the Data Processor, which may be carried out electronically or manually, is aimed exclusively at the execution of the activities indicated above, for which the data will be processed only if necessary, pertinent and not excessive.

The Data Processor is therefore prohibited from any further processing of such personal data, in particular if carried out for purposes other than those for which the data were provided, such as for example marketing, study and research.

The Data Processor will therefore be liable for any damages that may be caused to the rights, freedoms and dignity of the Interested Parties if he/she carries out processing for additional purposes not connected to the service provided or does not comply with the instructions provided.

ART. 2 - DURATION OF DATA PROCESSING

The processing of personal data is permitted to the Data Processor for the entire duration of the legal relationship, as specified in the introduction, without prejudice to the longer storage time of the data for the period strictly necessary for the completion of any administrative activities related to contractual obligations (reporting, verification, control, etc.).

The Data Processor is authorized to retain the data being processed for the time strictly necessary to carry out the agreed services; in particular, the Data Processor cannot retain paper or electronic copies of the data and documentation being entrusted, which must be returned if the conditions provided for by law or by the stipulated legal act are met or if this is in any case made necessary by the revocation of consent to the processing of data by the individual Interested Party.

The Data Processor also undertakes to promptly return the data to the Data Controller if requested by the latter. In any case, the Processor is required to delete all data contained in its physical and computerized archives, including those stored by the backup system, unless otherwise provided by law, at the end of the relationship.

At the end of the relationship, the Data Processor is also required to formally declare to the Data Controller via a specific PEC communication, within one month of the termination of the relationship, that he/she has carried out the aforementioned cancellation.

ART. 3 - TYPE OF PERSONAL DATA

The personal data processed by the Data Processor are:

☐Personal data (name, surname, gender, date and place of birth, tax code, residence, domicile, other)

☐Contact details (postal or email address, landline or mobile telephone number)

☐Data relating to identification/recognition documents (identity card, driving licence, CNS, other)

☐Login and identification data (username, password, customer ID, other…)

☐Payment data (bank account number, credit card details, other…)

☐Data relating to the provision of an electronic communication service (traffic data, data relating to Internet browsing, other…)

☐Profiling data

☐Location data

☐Data relating to criminal convictions and offences or related security or prevention measures

☐Data belonging to the special categories referred to in art. 9 of theEU Reg. 2016/679and, specifically:

□ health data
□ data relating to sexual life/sexual orientation
□ genetic data
□ biometric data
□ data relating to racial/ethnic origin
□ data relating to political opinions or religious/philosophical beliefs
□ data relating to trade union membership

ART. 4 - DATA SUBJETCS

The Controller is authorised to process personal data belonging to the following categories of subjects:

☐Employees

☐Consultants/Collaborators

☐Users/Contractors

☐Beneficiaries or assisted

☐Patients

☐Minors

☐Legal representatives (parents, support administrators, guardians, etc.)

☐Vulnerable people (e.g. victims of violence or abuse, refugees, asylum seekers)

☐Other (specify)____

Section II
Instructions of the Data Controller

ART. 5 - GENERAL OBLIGATIONS

The Data Processor is required to collaborate with the Data Controller to ensure compliance with the legislation on the protection of personal data, and in particular to process personal data:

- in compliance with the general principles of lawfulness, correctness and transparency, only if necessary and relevant to the execution of the entrusted processing and in any case for the minimum necessary period;
- in compliance with the principle of minimisation, in particular avoiding unnecessary duplications;
- by adopting adequate technical and organizational security measures, which ensure the protection of personal data and the protection of the rights, freedoms and dignity of the interested parties;
- making availableof the Data Controller any information necessary to demonstrate compliance with the obligations set out in this document, including that necessary toprovide, within 24 hours of the request, feedback to the requests of the interested parties and to the requests of the Authority for the protection of personal data, providing any information requested for this purpose;
- allowing any review, audit and control activity, including inspections by the Data Controller or another person appointed by the Data Controller with adequate prior notice;
- by communicating to the Data Controller, within 24 hours of becoming aware of it, any security incident or personal data breach referred to in point 12 of Article 4 of the GDPR, i.e. any security breach resulting in the accidental or unlawful destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed (data breach);
- promptly and proactively communicating to the Data Controller any information relevant to the protection of confidentiality and data protection, informing him immediately if he believes that an instruction given for the processing violates the rules on the processing of personal data;
- by forwarding to the Data Controller by 31 January of each year a report highlighting the state of the art of compliance with the provisions imparted by this act or by subsequent acts.

ART. 6 - OBLIGATIONS TO ADOPTION ADEQUATE TECHNICAL AND ORGANIZATIONAL MEASURES

The Data Processor also undertakes, in order to ensure a level of security appropriate to the risk, to adopt adequate technical and organizational measures, also in compliance with Article 32 of the GDPR, aimed at ensuring that:

- the processing of personal data is carried out only by its collaborators and in the event that it intends to avail itself, even for storage or processing activities through software, hardware or cloud information systems, of other subjects, the aforementioned indications are respected;

- the premises in which personal data are processed or stored or the devices used for their electronic storage present all the structural and technical security guarantees to prevent damage, loss or illicit acquisition of data by third parties;
- the confidentiality, integrity, availability and resilience of the systems and services used for the processing of personal data are ensured on an ongoing basis;
  (Optional part: maintain the following requirements only if required to be fulfilled by the Data Processor in the context of the underlying relationship):
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident is ensured;
- a procedure is in place to regularly test, verify and evaluate the effectiveness of the technical and organizational measures adopted to ensure the security of the processing of personal data;
- security measures consisting of pseudonymisation and data encryption techniques are adopted to prevent their immediate correlation with the interested party by subjects who do not need to know the identity;
- a specific log file is activated and maintained to record accesses and activities carried out by authorised persons;
  (End of optional part)
- the register of processing activities pursuant to paragraph 2 of Article 30 of the GDPR is prepared and kept up to date, identifying and recording the processing of personal data carried out on behalf of the Data Controller as well as the databases and archives managed with computer and/or paper supports necessary for carrying out the activities subject to delegation;
- all the measures provided for by the provision of the supervisory authority of 27 November 2008 relating to "Measures and precautions prescribed for the Data Controllers of processing carried out with electronic instruments in relation to the attributions of the functions of system administrator" are adopted.

ART. 7 - SUB-PROCESSORS OF THE PROCESSING REFERRED TO IN PARAGRAPH 2 OF ARTICLE 28 OF THE GDPR

(*Choose one of the two options - a) or b) - and delete the unused one entirely)*

to) In case of specific preliminary authorization:

The Data Processor may not use a sub-Processor to carry out the processing activities to be performed on behalf of the Data Controller without the prior specific written authorization of the Data Controller. The Data Processor shall submit the request for specific authorization at least …. days *(indicate the number of days, which may vary from 15 to 30, depending on the needs of the operating unit)* before using a sub-Processor, together with the information necessary to allow the Data Controller to decide on the authorization. The list of sub-processors shall be kept up to date.

b) In case of general written authorization:

The Processor has the general authorization of the Controller to engage sub-processors on the basis of an agreed list. The Processor shall specifically inform the Controller in writing of any intended changes to that list, concerning the addition or replacement of sub-processors, at least days in advance (please indicate the number of days, which may vary from 15 to 30, depending on the needs of the business unit) thereby giving the Controller sufficient time to object to such changes before engaging the sub-processor(s) in question. The Processor shall provide the Controller with the necessary information to enable him/her to exercise the right to object.

Where a Data Processor engages a sub-processor to carry out specific processing activities, the Data Processor shall enter into a contract that imposes on the sub-processor the same data protection obligations as those imposed on the Data Processor under these clauses. The Data Processor shall ensure that the sub-processor complies with the obligations to which the Data Processor is subject under these clauses and Regulation (EU) 2016/679.

Upon request of the Data Controller, the Data Processor shall provide the Data Controller with a copy of the contract entered into with the Sub-Processor and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the Data Processor may redact information from the contract before transmitting a copy.

The Data Processor remains fully responsible to the Data Controller for the fulfillment of the obligations of the Sub-Processor arising from the contract that the latter has stipulated with the Data Processor.The Data Processor shall notify the Data Controller of any failure by the Sub-Processor to comply with contractual obligations.

ART. 8 - FAILURE TO COMPLY WITH THIS ACT AND TERMINATION

Without prejudice to the provisions of Regulation (EU) 2016/679, if the Data Processor violates the obligations incumbent upon him by this Act, the Data Controller may instruct him to suspend the processing of personal data until the latter complies with this Act or the contract is terminated. The Data Processor shall promptly inform the Data Controller if, for any reason, he is unable to comply with this Act.

The Data Controller has the right to terminate the underlying relationship, with regard to the processing of data, if:

1) the processing of personal data by the Data Processor has been suspended by the Data Controller for violation of this Act and compliance with this Act is not restored within a reasonable time and in any casewithin one month of suspension;

2) the Data Processor substantially or persistently violates this Act or its obligations under Regulation (EU) 2016/679;

3) the Data Processor fails to comply with a binding decision of a competent judicial body or supervisory authority regarding its obligations under these Clauses or Regulation (EU) 2016/679;

The Data Processor shall have the right to terminate the underlying relationship, with respect to the processing of personal data, pursuant to this Act if, after having informed the Data Controller that its instructions violate Regulation (EU) 2016/679, the Data Controller insists on compliance with the instructions by the Data Processor.

ART. 9 - RETURN AND CANCELLATION OF PERSONAL DATA

The Data Processor, upon expiry of the underlying relationship or, in any case, in the event of termination - for any reason - of the effectiveness of this deed of appointment, except for the existence of a legal obligation that provides for its conservation, must interrupt all processing operations and must provide for the return of the processed data and the cancellation of any copies held.

Any copies, unless otherwise agreed upon upon termination of the relationship, must be destroyed within times compatible with any further needs that may arise; in this intermediate period between the end of the relationship and said deadline, the data will be retained by the Data Processor for security purposes only and will not be subject to further processing.

In the event of termination of the contract pursuant to Article 8 of this Act, the Data Processor shall, at the discretion 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 the retention of personal data. Until the data are deleted or returned, the Processor shall continue to ensure compliance with this Act.

In the event of a written request from the Data Controller, the Data Processor is required to issue a written certification of the cancellation operation, indicating the technical methods and procedures used for the cancellation.

In derogation from what is indicated in the previous points, the Data Processor shall retain said data if this is required by Union or State law until the term imposed by the legislation.

ART. 10 – DATA TRANSFER

Any transfer of personal data by the Data Processor to a third country or an international organisation may be carried out, in compliance with Chapter V of Regulation (EU) 2016/679, only with the prior indication and documented instructions of the Data Controller.

The Controller agrees that where the Data Processor engages a sub-processor to carry out specific processing activities (on behalf of the Controller) and these involve the transfer of personal data pursuant to Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor may ensure compliance with that Chapter V of Regulation (EU) 2016/679, in particular by using the 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 such standard contractual clauses are met.

ART. 11 - FINAL PROVISIONS

The parties acknowledge that this document constitutes the deed of appointment as Data Processor and each of its provisions shall be interpreted in a prevailing manner with respect to any other provision that may conflict and be contained in other documentation signed between the parties.

Failure to comply with the provisions regarding data processing and the instructions provided in this document constitutes an element of evaluation for the possible continuation or renewal of the underlying relationship.

This appointment does not imply any right, on the part of the Data Processor, to a specific compensation or indemnity or reimbursement nor to an increase in the compensation foreseen for the provision of the service.

The parties reserve the right to modify or integrate this deed of appointment should this prove necessary.

For anything not expressly provided for, please refer to the general provisions in force applicable to the protection of personal data.

Read, confirmed and signed

THE DATA CONTROLLER
IRCCS Policlinico San Martino
General Director

____

For acceptance
THE DATA PROCESSOR

____

General Director / other Legal Representative

____