updated 14/07/2025

Annex 1 to the Data Processing Agreement (DPA) – Nanosystems S.r.l.

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES (TOM)

A) Organizational measures:

· Appointment of sub-processors: Nanosystems may, as data processor, use sub-processors to carry out its activities in accordance with the contract signed by the user and the DPA.
The sub-processors were communicated at the time of signing the aforementioned contract and provide sufficient guarantees of adequacy in relation to the protection of the rights and freedoms of the data subjects.
Should Nanosystems decide to use additional sub-processors or replace the previous ones, modifying the relevant agreements, it will request authorization from the Data Controller in accordance with Article 28 of Regulation (EU) 2016/679 (GDPR).

· Appointment of Authorized Persons: appointment issued to expressly designated natural persons, authorized to perform, through the assignment of specific tasks and functions, processing operations by the Data Controller or the Data Processor, under their authority; such appointments are specifically recorded in the data accessibility register held by Nanosystems.

· Paper storage in secure locations: documents containing particularly sensitive personal data, when processed in paper format, are stored in secure physical containers (e.g., locked cabinets or drawers) located in restricted access areas.
Access to these documents is restricted to personnel, expressly authorized by the Company.
The Company adopts and maintains a register of physical access to these containers in order to ensure the traceability of access and compliance with the principles of integrity and confidentiality provided for in Article 32 of the GDPR.

· Company Security and Privacy Policy: Nanosystems has adopted an internal policy on the protection of personal data with the aim of protecting the personal data processed and preventing the risks associated with processing, in accordance with the principles established by European and national privacy legislation.
The policy define the internal procedures for compliance with the obligations set out in Legislative Decree No. 196 of June 30, 2003, as amended (Privacy Code), as well as the GDPR, with reference to the processing of personal data within the company.
In particular, it identifies:

- the internal operating provisions applicable to processing carried out by the Company;
- the roles and responsibilities of the persons involved;
- the obligations to be observed in accordance with the decisions and measures of the Data Protection Authority.

In addition, Nanosystems has adopted an internal information security policy aimed at defining the organizational, technical, and procedural measures to ensure the confidentiality, integrity, and availability of the data processed.

· Credential modification procedure: Nanosystems adopts a secure procedure for managing and modifying access credentials to company services linked to the corporate domain.
All employees access the systems through named user accounts; the relevant passwords can only be reset by the Security Manager or by expressly authorized personnel.
Nanosystems maintains aninternal policy for the generation of credentials, which establishes:

- minimum complexity requirements (length, special characters, capital letters, numbers);
- prohibition on reusing recent passwords;
- mandatory expiration of credentials every 90 days;
- the obligation to change passwords immediately in the event of suspected unauthorized access.

These measures apply to all internal services connected to the company domain, including email tools, cloud environments, VPNs, administration and remote management tools.

· Data breach procedure: Nanosystems has prepared a Data Breach Management Manual, which aims to define roles, responsibilities, and the main operating procedures adopted to protect personal data and manage the risks involved in its processing, in accordance with the principles defined by the GDPR. In the event that a person belonging to Nanosystems' data protection governance or one of the other departments of the company detects an accidental loss of data (i.e., loss of a PC, USB, or sending emails to the wrong recipients) or a fraudulent attack on the integrity of its systems or any breach of confidentiality or integrity or availability, they shall promptly notify the Data Controller.
There is a procedure for managing detected breaches that may affect the personal data of data subjects, based on the distribution of roles according to competence, the verification of potential damage and the assessment of the risk resulting from the personal data breach, the management of the countermeasures to be taken, as well as the method of communication to the Customer and the adoption of the related obligations under the privacy legislation.

· Procedure for data subjects' rights: if Nanosystems receives requests from data subjects regarding the exercise of their rights in relation to personal data that it analyzes and processes on behalf of the Data Controller, it shall forward such requests to the Data Controller as soon as possible, who will handle them. The Data Processor, i.e. Nanosystems, shall assist the Data Controller by providing it with all information relating to the services managed by Nanosystems under this agreement and shall invite the data subject to contact the Data Controller in order to exercise their rights, emphasizing its position as Data Processor. Nanosystems undertakes to manage the

rights of data subjects in an appropriate manner.
In the event that the Data Controller must respond to requests from data subjects regarding the exercise of their rights with reference to personal data covered by this agreement, Nanosystems will provide the requested information, if in its possession, in accordance with this agreement, in relation to the services purchased and used by the Data Controller. In any case, the latter will process the request directly.
In the event that the Data Controller needs to comply with requests for the portability of personal data, the Data Processor shall provide, solely for the services purchased by the Data Controller, the information necessary to extract them in a format that complies with privacy legislation and if this is reasonably possible. If the Data Controller requests essential technical assistance to carry out the aforementioned extraction, Nanosystems will consider its technical feasibility and agree with the former on the relevant procedures and costs to be borne by the Data Controller.

· Instruction and training of authorized persons: The Data Processor shall provide practical training, following theory and an assessment test of the skills acquired, in which all critical issues that may arise during work and could lead to a data incident are simulated in a safe environment.

· Reviews and updates: These technical and organizational measures are subject to periodic review. Any updates will be communicated promptly to the Data Controller. The measures will be adapted in line with the evolution of risks and available technologies.

B) Technical measures

· Authentication: The processing of personal data by electronic means is permitted to persons in charge of processing who have authentication credentials that allow them to pass an authentication procedure relating to a specific processing operation or set of processing operations. Each person in charge of processing is assigned or associated with one or more authentication credentials. The instructions given to the persons in charge require them to take the necessary precautions to ensure the confidentiality of the confidential component of the credentials and the diligent custody of the devices in their possession and for their exclusive use. Instructions are given to the persons in charge not to leave the electronic device unattended and accessible during a processing session.

· Authorization: Only authorized persons have access to the system that collects and processes personal data. Nanosystems uses multiple levels of authorization when granting access to systems. Authorizations are updated regularly.

· Data encryption: Nanosystems encrypts the information obtained from personal data so that it cannot be understood by third parties, thereby ensuring confidentiality. These systems are based on algorithms and computer protocols that meet international standards.

· Separation: The practice of keeping systems, data, or environments separate to limit access and reduce risks.

· Firewall: Nanosystems uses physical and logical perimeter protection devices for its IT infrastructure to prevent cyber attacks and external intrusions by third parties.

· Business Continuity: Plan and solutions for restoring data and systems following a catastrophic event.

· Disaster Recovery: Strategies and measures to ensure business continuity even in the event of adverse events (failures, attacks, disasters).

· Intrusion detection: Nanosystems uses tools that can monitor traffic entering and leaving a network to detect any suspicious activity or cyber attacks.

· *Pseudonymization:* Nanosystems uses pseudonymization where it does not affect the efficiency of the procedures and/or where data protection is necessary for the purpose of the processing. Where possible, anonymization is used as part of the statistical analysis process. Nanosystems follows a procedure to assess internal data sharing and uses pseudonymization to limit the use of personal data for certain purposes.

· Backup and recovery: The Data Processor provides for daily automated backups and performs periodic tests, which are recorded.

· Verification of security measures: Nanosystems performs security audits on a regular basis to verify the effectiveness of technical and organizational measures on an ongoing basis.

· Data deletion and return: The Data Processor has established standard procedures for the secure return or deletion of data upon termination of the contractual relationship.