ThermoFisher SCIENTIFIC

The world leader in serving science

THERMO FISHER SCIENTIFIC
TECHNICAL AND ORGANIZATIONAL MEASURES (TOMS)

This Annex describes the TOMs that the Processor shall, as a minimum, maintain to protect the security of the Personal Information processed under the Agreement and to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems. The Processor shall provide records of the implemented TOMs defined below to facilitate audits and to prove compliance with the Processor's obligations.

Access Control to Processing Areas

The Processor shall implement suitable measures in order to prevent unauthorized individuals from gaining access to the data processing equipment used for the data processing. This requires:

- establishing security areas;
- protection and restriction of access to processing areas;
- securing the data processing equipment;
- establishing access authorizations for staff and third parties, including the respective documentation;
- regulations on key cards;
- restriction on key cards;
- all access to the data centre where the Personal Information are hosted is logged, monitored, and tracked; and
- the data centre where the Personal Information are hosted is secured by a security alarm system, and other appropriate security measures are implemented.

Access Control to Data Processing Systems

The Processor shall implement adequate measures to prevent its data processing systems from being used by unauthorized persons. This requires:

- identification of the terminal and/or the terminal user to the Processor systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes;
- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions;
- staff policies in respect of each staff access rights to the Personal Information (if any), informing staff about their obligations and the consequences of any violations of such obligations, ensuring that staff will only access the Personal Information and resources required to perform their respective duties and training of staff on applicable data protection regulation and the respective responsibilities;
- all access to data content is logged, monitored, and tracked; and
- use of state-of-the-art encryption and pseudonymization technologies.

Access Control to Use Specific Areas of Data Processing Systems

The Processor shall ensure that the individuals entitled to use its data processing system are only able to access the Personal Information within the scope and extent covered by its access permission (authorization) and that the Personal Information cannot be read, copied or modified or removed without authorization. This requires:

- staff policies in respect of each staff member's access rights to the Personal Information;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the Personal Information and at least yearly monitoring and updating of authorization profiles;

- effective and measurable disciplinary action against individuals who access the Personal Information without authorization;
- release of Personal Information limited to authorized individuals;
- control of files, including he controlled and documented destruction of Personal Information;
- policies controlling the retention of back-up copies; and
- use of state-of-the-art encryption pseudonymization technologies.

Transmission Control

The Processor shall implement adequate measures to prevent the Personal Information from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This requires:

- use of state-of-the-art firewall and encryption and pseudonymization technologies to protect the gateways and pipelines through which the Personal Information travels;
- as far as possible, all data transmissions are logged, monitored and tracked; and
- monitoring of the completeness and correctness of the transfer of Personal Information (end-to-end check)

Input Control

The Processor shall implement adequate measures to ensure that it is possible to check and establish whether and by whom the Personal Information have been put into the data processing systems or removed from such systems. This requires:

- a policy for the authorization to put Personal Information into memory, as well as for the reading, alteration and deletion of stored Personal Information;
- authentication of the authorized personnel; individual authentication credentials such as user IDs that, once assigned, cannot be re-assigned to another individual;
- protective measures for the Personal Information input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords) of at least eight characters or the system maximum permitted number and modification at first use and thereafter at least every 90 days in case of processing of sensitive data;
- implementation of a policy according to which all staff of the Processor who have access to the Personal Information processed for the Controller shall reset their passwords at a minimum once in a 180-day period;
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user ID's (requirement to re-enter password to use the relevant workstation) that have not been used for a significant period of time;
- automatic deactivation of user authentication credentials (such as user IDs) in case the person is no longer authorized to access the Personal Information or in case of non-use for a substantial period of time (at least six months), except for those individuals authorized solely for technical management
- proof of the input restrictions and authorizations by the Processor; and
- electronic recording of entries.

Job Control including processes for regularly testing, assessing and evaluating of the effectiveness of TOMs in order to ensure the security of the processing

The Processor ensures that the Personal Information may only be processed in accordance with written instructions issued by the Controller. This requires:

- binding policies and procedures for the Processor’s employees, subject to the review and approval of the Controller.

The Processor ensures that if security measures are implemented by third parties it will obtain a written description of the actions taken to guarantee compliance of the measures with the requirements of this Annex. The Processor shall further implement adequate measures to monitor its system administrators and to ensure that they act in accordance with instructions received under the Agreement. This requires:

- individual appointment of system administrators;
- adoption of adequate measures to register system administrators' access logs and to keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess conformity with the assigned tasks, the instructions received by the Processor and applicable data protection laws; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and assigned tasks for providing this to the Controller upon request.

Availability Control including measures to restore the availability and access to the Data in a timely manner in the event of a physical or technical incident

The Processor shall implement adequate measures to ensure that the Personal Information are protected from accidental destruction or loss. This requires:

- infrastructure redundancy to ensure data access is restored within maximum seven days and backup performed at least weekly;
- tape backup is stored off-site and available for recovery in case of failure of SAN infrastructure for database server;
- only the Controller may authorize the recovery of backups (if any) or the transfer of Personal Information outside of the location where the physical database is held, whereby in case of transfer the security measures shall be adjusted to avoid loss or unauthorized access to the Personal Information, when transferred;
- regular check of all the implemented security measures described in the Agreement at least every six months;
- removable media containing sensitive or judicial data shall be destroyed or made unusable when not used anymore; alternatively, the data media may be re-used if data previously stored on that media cannot be re-constructed by any technical means; and
- any detected security incident is recorded, alongside the executed data recovery procedures, and the identification of the individuals who carried them out.
-

Separation of Data

The Processor shall implement adequate measures to ensure that Personal Information collected for different purposes can be processed separately. This requires:

- access to data is separated through application security for the appropriate users (logical separation);
- modules within the Processor's data base allow the separation of data regarding their purpose, i.e. by functionality and function; and
- at the database level, the Personal Information is stored in different normalized tables, separated per module or function they support; interfaces, batch processes and reports are designed exclusively for specific purposes and functions, to ensure that the Personal Information collected for different purposes are processed separately
- measures of pseudonymization or encryption of Personal Information.

ANNEX B:

Definitions and interpretation

In these TOMS:
"**Affiliate**" means any legal entity that directly or indirectly controls, is controlled by, or is under common control of, a contract party. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of a contract party.

"**Data Protection Legislation**" means any data protection or privacy-related laws and regulations that regulate the processing of Personal Information (e.g. EU General Data Protection Regulation 2016/679 (the 'GDPR') and the United States Health Insurance Portability and Accountability Act Public Law 104-191 ('HIPAA'), the California Consumer Privacy Act (CCPA) and any other applicable data protection laws and regulations including but not limited to those listed in Annex E with respect to specific jurisdictions.

The terms "**data controller**", "**data processor**" and "**appropriate technical and organizational measures**" shall be interpreted in accordance with applicable Data Protection Legislation in the relevant jurisdiction.

"**Individual**" means the identified or identifiable individual to whom the Personal Information relates. Individual should be understood to include any related definitions used in Data Protection Legislation (e.g. 'data subject' as defined in the GDPR).

"**Parties**" means Thermo Fisher and Vendor.

"**Personal Information**" shall be construed broadly as any information relating to an identified or identifiable Individual. This information may include name, address, e-mail address, telephone number, age, gender, family information, profession, education, salary, credit card numbers and other attributes that identify an individual. Personal Information should be understood to include any related definitions used in Data Protection Legislation (e.g. 'personal data' as defined in the GDPR, 'protected health information' or 'PHI' as defined under HIPAA, or 'Personal Identifiable Information' or 'PII' as defined under the CCPA and various other US state laws). This DPA is not intended to confer additional legal rights on Individuals beyond those provided for in applicable law.

"**Privacy Breach**" means any incident, including a breach of data security, leading to the accidental or unlawful destruction, loss, alteration, damaging, or unauthorized disclosure or acquisition of, or access to the Personal Information that Vendor processes in the course of providing Services, and any other event which would have to be notified to a data protection authority and/or Individuals under Data Protection Legislation, or any breach thereof or of this DPA by Vendor.

"**Process**", "**processed**" or "**processing**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure and disposal.

"**Sensitive Personal Information**" means Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation, or Personal Information relating to criminal convictions or offences. Sensitive Personal Information should be understood to include any related definitions used in Data Protection Legislation (e.g. 'special categories of personal data' as defined in the GDPR and 'PHI' as defined in HIPAA, CCPA and other US state statutes).

"**Services**" means the services to be provided by Vendor to Thermo Fisher pursuant to and as further set out in the Agreement.