This document is applicable when in Effective status

Effective Date (GMT) : 30 Sep 2025

Owning Department : Digital Digital CyberSecurity

Previous Document Number : SD-001458

Document Author Approval Task Approve	Leila BOUSFOUL, Cyber Security Expert Document Author Approval 30-Sep-2025 14:04:52 GMT+0000
Approval Task Approve	Jean-Yves POICHOTTE, Global Head of Cyber Security Risk & Compliance Approval 30-Sep-2025 14:33:50 GMT+0000
Approval Task Approve	Emilie DESCHAMPS, Risk Advisory Lead â€“ Cyber and Tech MS Quality Assurance Approval 30-Sep-2025 14:35:53 GMT+0000

Table of Contents

1. CYBERSECURITY MEASURES

This Appendix sets forth SANOFI's cybersecurity measures applicable to the CONTRACTOR pursuant to the agreement entered into between the CONTRACTOR and SANOFI (the "Agreement"). CONTRACTOR must comply with such measures at its own costs.

1. DEFINITIONS

When the first letter is capitalized, the terms used herein have the meaning set out in the Agreement, unless otherwise specified herein.

Artificial Intelligence "AI" or "AI System" means a digital artefact (business application, analytics dashboard, software as medical device, mobile application, etc.) that uses relevant data and AI learning techniques to generate insights for business use. The insights can be in the form of prediction, recommendation, new content, autonomous decision or manifest as automated actions.

Audit Trail(s) means a chronological recording of events, such as creation, modification, deletion and access to record or e-record, that allows reconstruction of the course of events and indicates who created, accessed, changed or deleted data and why.

Deliverables means all materials created, generated, designed, prepared or developed by Contractor within the scope of the Agreement, including, but not limited to any designs, databases, files, documents, training materials, outputs, reports, notes, study or analytical documents, minutes or reports, trademarks, digital development, specifications, updates and version installations of programs and/or interfaces designed, created, submitted, developed, written in object code or source code for SANOFI, whether or not protected or capable of being protected by intellectual property applicable laws.

Disaster means any event that causes, or is likely to cause, an adverse effect on the performance of the Agreement including interruption, destruction, quality reduction or other loss of operational capacity of CONTRACTOR or CONTRACTOR's Personnel.

Environment means SANOFI's or CONTRACTOR's current computing and telecommunications environments (consisting of hardware and software) used within the framework of the Agreement and/or potentially interfaced with the Equipment and/or Deliverables.

Equipment means all equipment, terminals, infrastructures, related hardware and software, including, as applicable, systems (applications, databases, processing units, personal computers and other processors, controllers, storage devices, printers, phones, other peripherals and input as well as output devices, and other tangible mechanical and electronic equipment intended for the processing, input, output, storage, manipulation and retrieval of data.

IT Change(s) means any actual or proposed change to the nature, level and extent/scope of an Equipment.

Personal Data has the meaning set forth in the Agreement and/or the Data Processing Agreement if applicable.

Professional Standards means, in relation to any particular undertaking or task included, contemplated or envisaged for the performance of the Agreement, those standards, practices, methods and procedures conforming to all applicable laws that must be complied with according to the nature of the Agreement and/or the Sanofi Data and the presence of Personal Data, and followed with the highest degree of skill, diligence, prudence and foresight that may be reasonably expected of a contractor completing similar activities or acting in similar circumstances, and all this in a manner that complies with recognized international standards.

Sanofi Data means all data, information, text, drawing, picture, video, sound, statistics, analysis and other materials embodied in any form relating to SANOFI or its Affiliated Companies and/or users (where relevant) and/or Deliverables, which may be supplied by SANOFI or its Affiliated Companies (and/or its users) (including Personal Data) and/or to which CONTRACTOR has access to, generates, collects, processes, stores or transmits and associated Audit Trail in the course of performing the Agreement.

Security Laws means all applicable regulations addressing cyber security including but not limited to (i) Network and Information Security 2 Directive (Directive (EU) 2022/2555 ("NIS 2 Directive") along with all local laws and regulations implementing such directive and (ii) Cyber Resilience Act. For clarity, it is understood that the Security Laws, as defined in this Exhibit, are an integral part of the definition of "applicable laws," as provided in the Agreement if applicable.

Vulnerability means any asset weakness that can be exploited to cause harm to the SANOFI organization**.** Vulnerabilities can be Critical or non-Critical.

Critical Vulnerability means every Vulnerability with a Common Vulnerability Scoring System (CVSS https://www.first.org/cvss/specification-document) score greater than or equal to nine (9) or Vulnerabilities with a lower CVSS score under specific conditions, including without limitation, if such Vulnerabilities are massively exploited and deemed to represent a significant risk to SANOFI's organization.

Non-Critical Vulnerability means any Vulnerability which is not Critical Vulnerability as defined above.

2. GENERAL SECURITY OBLIGATIONS

CONTRACTOR undertakes to put in place all necessary technical, organizational and/or security measures to comply with applicable laws and Security Laws, including in terms of training, reporting obligations, risk assessments or resilience plans. If the requirements set forth in the present document are less stringent than those of the Security Laws, the most stringent terms of the Security Laws shall prevail.

Information security contact. CONTRACTOR shall designate and communicate to SANOFI as single point of contact an IT security responsible individual, (along with a back-up assistant) in charge of the security measures listed herein.

Change management. CONTRACTOR shall implement an IT Change management process to identify changes to the nature, level and extent/scope of any IT system that could impact compliance with any of the obligations set forth herein and immediately report any deviation or breach to SANOFI.

Information Security and Integrity Program. CONTRACTOR shall implement and maintain a comprehensive, "Information Security & Integrity Program" relevant to the Agreement, consistent with Professional Standards, and containing policies and procedures, administrative, technical, and physical safeguards and best practices in order to ensure the security of the Equipment and Sanofi Data.

Security Assurance Plan. To the extent CONTRACTOR provides Application and infrastructure services, CONTRACTOR shall implement and maintain a comprehensive security assurance plan describing how CONTRACTOR will implement, when applicable, each security measure listed in this Appendix. The Security Assurance Plan shall be validated by SANOFI prior to the performance of the Agreement.

Subcontractors. CONTRACTOR shall flow down all cyber security obligations or least substantially similar obligations as those defined in the Agreement to its subcontractors and in particular those that have access to or processing Sanofi Data and/or are involved in the delivery of Deliverables and Services.

3. ACCESS MANAGEMENT

Access to Sanofi Data. To the extent that CONTRACTOR has access to Sanofi Data, CONTRACTOR shall (i) grant access only to authorized CONTRACTOR personnel with adequate credentials (ii) keep available to SANOFI a regularly reviewed registry of Contractor's and/or Subcontractor's authorized personnel, (iii) keep access and activities logs and Audit Trails.

Access to SANOFI's Environment*. To the extent that CONTRACTOR has access to SANOFI's Environment, CONTRACTOR undertakes (i) to comply in particular with SANOFI policies pertaining to the delivery, use and revocation of the identifier(s) and password(s) provided by SANOFI (collectively the "Access Codes"), (ii) to keep all Access Codes provided by SANOFI strictly confidential, (iii) use them only for the purpose of and duration necessary for the performance of the Agreement. CONTRACTOR shall inform immediately SANOFI if it has reasons to believe that such Access Codes have been compromised or are used by third parties. All actions performed through the Access Codes shall be deemed performed by CONTRACTOR. Contractor must bring its own strong MFA capabilities (FIDO2 hardware key or Microsoft Authenticator). SANOFI will not provide smartphones or FIDO2-compatible hardware**.**

Access to SANOFI's premises. To the extent CONTRACTOR is given physical access to Sanofi's premises (including hosting premises of Sanofi Data), CONTRACTOR shall (i) ensure that only authorized Personnel is given access (ii) carry out regular physical access rights reviews.

Remote Access. To the extent CONTRACTOR implements, maintains, or administers any kind of SANOFI's Equipment remotely, CONTRACTOR shall (i) comply with SANOFI's procedures pertaining to remote access as communicated by SANOFI (ii) only use the remote access means provided by SANOFI.

Monitoring. CONTRACTOR acknowledges that SANOFI may monitor CONTRACTOR's activity on SANOFI's Environment in accordance with applicable laws as set out in SANOFI's Information Technology (IT) and Solutions Usage Policy as communicated by SANOFI.

Passwords Protection. CONTRACTOR shall ensure that its password policy meets Professional Standards (such as "Password Protection Policy" from SANS Institute or "DAT-NT-001/ANSSI/SDE/NP").

On-site interventions. To the extent the performance of the Agreement implies on-site interventions, CONTRACTOR shall (i) use SANOFI's resources only for the performance of the Agreement, (ii) comply with SANOFI's policies and procedures pertaining to cybersecurity, including on-site Equipment declaration, prior security scans and anti-virus checks, (iii) only use Sanofi Data within SANOFI's information system, unless approved by SANOFI, (iv) use only SANOFI-managed Equipment to connect to the Deliverables. In addition, and unless authorized by SANOFI, CONTRACTOR shall refrain from (i) connecting roaming laptops to SANOFI's Equipment and from (ii) using SANOFI's local area network.

4. PERSONNEL

Acceptable Use Policy. CONTRACTOR shall implement an acceptable use policy (covering teleworking where applicable) that its personnel including those of its Subcontractors shall comply with before accessing CONTRACTOR's Equipment and/or Sanofi Data.

Ongoing control. CONTRACTOR shall ensure adequate control over the information security tasks delegated to its Personnel and/or subcontractors on an ongoing basis.

Information security training and awareness program. CONTRACTOR shall implement and monitor attendance to training programs for its Personnel regarding its security obligations as required by their job responsibilities and all applicable laws and Professional Standards.

Personnel departure. In case of CONTRACTOR Personnel departure, CONTRACTOR shall implement adequate security measures and in particular undertake that (i) credentials have been deactivated, (ii) SANOFI's Equipment and Sanofi Data have been returned, (iii)

any Sanofi Data stored on a Personnel's computer, laptop or external media is securely wiped, immediately upon such departure.

5. SANOFI DATA SECURITY AND PORTABILITY

Usage limitation. To the extent CONTRACTOR hosts, processes, transmits or collects Sanofi Data, CONTRACTOR shall (a) process Sanofi Data exclusively as instructed or authorized by SANOFI under the Agreement and for as long as it is strictly necessary as determined by the Agreement (b) restrict Sanofi Data's access only to authorized CONTRACTOR'S personnel, SANOFI or other entities authorized in advance in writing by SANOFI, c) use Sanofi Data solely for the benefit of Sanofi and d) keep available to SANOFI log records keeping track of all actions and/or attempted actions performed on those data.

Segregation. To the extent Sanofi Data or Deliverables (including any AI Systems processing such Data) are hosted on infrastructure owned or operated by the CONTRACTOR, the CONTRACTOR shall ensure that Sanofi Data is stored in a physically or logically separate environment from all other execution and storage environments.

Storage. CONTRACTOR must ensure the security, confidentiality, availability, and integrity of the Sanofi Data stored on databases, servers, or other forms of non-mobile devices against disclosure, destruction, loss, theft, alteration, access and unauthorized use and access, whether from accidental or malevolent, and all anticipated forms of compromise, whether by use of state-of-the-art encryption mechanisms, logical access controls or other robust safeguards.

Encryption. Wherever the Sanofi Data is stored, CONTRACTOR shall ensure to use encrypted format, in accordance with state-of-the-art cryptography mechanisms. CONTRACTOR shall ensure that all SANOFI Data is encrypted in transit and at rest.

Back-up. CONTRACTOR shall perform on a regular basis, at least once per day, having two (2) backup copies at different remote locations of (i) Sanofi Data, (ii) associated Audit Trail, and (iii) system configuration. CONTRACTOR must ensure that back-up is performed in accordance with cybersecurity Professional Standards and in particular that back-up copies (i) are encrypted and protected from crypto-locking attacks, (ii) are stored on reliable media during the duration imposed by applicable laws and/or by SANOFI in the Agreement or any documentation provided to CONTRACTOR, (iii) maintain the integrity and accuracy of Sanofi Data (iv) so it can be restored promptly at any time. CONTRACTOR shall perform restoration test on (i) Sanofi Data, (ii) associated Audit Trail, ad (iii) system configuration at least every year and provide, upon request, documented evidence to SANOFI in this respect.

Datacenter Location. CONTRACTOR shall communicate to SANOFI information security point of contact all datacenter locations used for the hosting of the Sanofi Data, including those used for backups, prior to the performance of the Agreement.

Portability. In accordance with the EU Data Act and with respect to data processing services (including cloud services), CONTRACTOR shall ensure, without any additional

charge, that SANOFI can switch at any time to another provider quickly and smoothly, and without losing any Sanofi Data or application functionality. CONTRACTOR shall set up (i) all operations that are necessary to facilitate switching and data egress, including in terms of interoperability, and (ii) providing open interfaces and, at a minimum, means to export Sanofi Data in a commonly used and machine-readable format. Upon SANOFI's request, SANOFI will provide technical specifications to the CONTRACTOR to securely transfer Sanofi Data (i.e. SANOFI secured environment).

Destruction. CONTRACTOR shall regularly review Sanofi Data to determine whether such Sanofi Data are still required for compliance with applicable laws or for the performance of the Agreement or if they should be deleted. CONTRACTOR shall provide evidence of Sanofi Data deletion upon SANOFI or its Affiliated Companies' request.

6. EQUIPMENT'S SECURITY AND SECURE DEVELOPMENT

Risk assessment plan. To the extent the performance of the Agreement includes Equipment (hardware or software), CONTRACTOR shall provide and implement an assessment of the internal and external risks to the security of the Deliverables or Sanofi Data, including identification and evaluation of Vulnerabilities to CONTRACTOR's Equipment. Such an assessment shall be performed at each major release of its Deliverables.

Cyber Protection and Monitoring. CONTRACTOR shall ensure at all times that the Deliverables and any CONTRACTOR's Equipment are at least secured through antivirus and Endpoint Detection and Response solution (EDR) managed and monitored by a Cyber Security Operation Center. The working hours of the Cyber Security Operation Center shall cover the period during which at least one workstation is connected to the CONTRACTOR network.

Secure development. To the extent the Deliverables include development or integration, CONTRACTOR shall implement adequate security measures all along the development lifecycle consistent with (i) the OWASP framework (Open Web Application Security Project) and/or (ii) a recognized cybersecurity framework for secure application development and (iii) SANOFI's standards listed below.

Such measures shall include but are not limited to (i) cybersecurity maintenance contracts with subcontractors, (ii) regular source code review and Vulnerability watch and tests, in particular before move to production (iii) regular patches and updates of software components (including software and container open source packages), (iv) segregation of the development environment(s) from the production environment(s), (v) management of access rights to source code and Sanofi Data, (vi) product and configuration hardening, including deactivation of unused or outdated functionalities and any type of libraries, change of default credentials including admin passwords, exclusion of uncontrolled source code (vii) control of configuration changes, (viii) exclusive use of only non-production and dummy data in the development and test environment, unless authorized by SANOFI.

Support and maintenance. CONTRACTOR shall ensure at all times that the Deliverables, any component of the solution and/or SANOFI's Equipment (i) are maintained and supported through their subsequent updates and upgrades, (ii) have all their component with version no later than N-1, N representing the last up-to-date version of each component, (iii) are maintained compatible with all the supported versions of SANOFI's components and (iv) are free from any publicly known vulnerability that may impact SANOFI security. CONTRACTOR shall (i) keep SANOFI informed of IT Changes brought to the Deliverables before their release, (ii) notify SANOFI at least a thirty (30) day before any update, (iii) notify SANOFI of the Deliverables end-support/maintenance dates (including all third-party components) at least one year in advance.

Without prejudice to the foregoing, CONTRACTOR shall (i) implement at all times a security patching process and apply the latest security patches, and (ii) change passwords for all accounts managed by CONTRACTOR in accordance with SANOFI's password policy as communicated by SANOFI.

Watch process. CONTRACTOR shall keep itself informed on threats and Vulnerabilities of the products and technologies implemented on the Equipment it provides or maintains, based on public or private information (including Computer Security Incident Response Team CSIRTs, and Equipment manufacturer's websites).

Vulnerability remediation. In case of discovery of a Vulnerability, CONTRACTOR shall deploy a remediation solution (i) within a maximum of one (1) month for Non-Critical Vulnerability and (ii) within three (3) calendar days for a Critical Vulnerability. Where not feasible, CONTRACTOR shall make available to SANOFI, within a maximum of three (3) calendar days from Critical Vulnerability discovery, a temporary palliative solution at no additional cost and offering equivalent performance and functionality. A definitive solution to the Critical Vulnerability must be provided to SANOFI within a maximum of ten (10) calendar days.

7. INFRASTRUCTURE SECURITY

SANOFI hosting infrastructure. To the extent the goods and/or services and/or Sanofi Data are hosted on infrastructure owned or managed by SANOFI, CONTRACTOR acknowledges that (i) the operating system will be a standard SANOFI image with hardened configuration, (ii) SANOFI Equipment is secured through, notably, antivirus, endpoint detection and response, local password management tool, software distribution agent, filtering and segmentation tools (Firewall, VLAN, etc.) and (iii) compatible systems are integrated into a WINDOWS active directory domain managed by SANOFI.

8. SECURITY INCIDENT MANAGEMENT

Detection. CONTRACTOR shall implement adequate procedures and technical measures to detect, track and keep records of all confirmed, attempted or threatened events, whether accidental or malevolent, leading to (i) the unauthorized disclosure, access, use, encryption, reproduction, deletion, loss, theft, alteration, or transmission of Sanofi Data, (ii) the

unauthorized access (physical or logical), theft or damage to SANOFI's Equipment controlled by CONTRACTOR, (iii) a disruption of the performance of the Agreement and/or Sanofi Data integrity, functionality or availability, and/or (iv) a breach or potential breach by CONTRACTOR of its security obligations (collectively "Security Incident").

Notification. CONTRACTOR shall report to SANOFI, within a maximum of twenty-four (24) hours after its discovery, any Security Incident or any other event that requires notification under applicable laws. Such report shall remain confidential and contain all information required or useful to assess the impact of the Security Incident and implement mitigation measures.

Remediation and mitigation. CONTRACTOR must alert SANOFI as soon as it has identified any suspected Security Incident that might impact SANOFI. CONTRACTOR shall mitigate Security Incidents by following an incident management process and adequate response plan (including prevention of future similar events) at its own costs. CONTRACTOR shall keep SANOFI informed on a regular basis of the progress of its investigation and response plan, until the Security Incident has been effectively and totally resolved.

Cooperation. CONTRACTOR shall fully cooperate with SANOFI in case of a security investigation regarding potential breaches of its obligations.

Disaster recovery and business continuity. To the extent that the performance of the Agreement may be subject to any business continuity breach or Disaster, or unscheduled unavailability, CONTRACTOR shall make sure and inform SANOFI that the performance of the Agreement can be resumed, including through alternative measures. CONTRACTOR shall keep informed and cooperate with SANOFI regarding the unavailability of the Deliverables (including causes, impact, estimated duration) & provide upon request, documented evidence to SANOFI in this respect.

9. QUANTUM RISK MANAGEMENT

CONTRACTOR shall anticipate and implement all necessary measures within the agreed timelines with SANOFI to ensure that all algorithms and protocols used in the performance of the Agreement are resistant to quantum computing attacks. This includes, but is not limited to, the use of post-quantum cryptographic algorithms as recommended by recognized standards bodies such as NIST.

10. AUDITS AND CONTROLS

Annual Information Security audit. Without prejudice to SANOFI's audit rights and remedies as per the Agreement, each calendar year, CONTRACTOR shall engage at its own costs an independent and nationally recognized audit firm to conduct a security technical configuration audit and penetration tests for internet exposed services. Upon SANOFI's request, CONTRACTOR shall provide a copy of audit reports and any documentation related to past audits or certifications. In addition, SANOFI shall be entitled

to audit CONTRACTOR, its subcontractors and their systems to monitor compliance with this Appendix.

Client-Initiated Security Assessments. If CONTRACTOR's or its subcontractor's systems or infrastructures are used to provide the Services, SANOFI may, at its own expense and without prior notice, conduct or commission remote or on-site security audits or penetration tests through a third party bound by confidentiality. These assessments are intended solely to verify cybersecurity compliance and the protection of SANOFI Data and Systems, without testing system resilience or disrupting normal operations.

Certification. CONTRACTOR shall provide relevant independent certification recognized by SANOFI (ISO27001 or SOC2 Type2) and maintain this certification during the term of the Agreement. If the CONTRACTOR is not able to provide and maintain such certification, CONTRACTOR shall perform at its own costs the SANOFI's standard vendor assessment through evidence-based questionnaire and maintain their assessment all along the term of the Agreement. If the results of the completion of such questionnaire are not meeting SANOFI's standards, reperform this assessment each calendar year until SANOFI's standards are satisfied following mitigation action & improvement plan.

11. ARTIFICIAL INTELLIGENCE

AI Security. CONTRACTOR shall promptly inform SANOFI's relevant point of contact if the CONTRACTOR is using, relying on or planning to use or rely on AI System in the performance of the Agreement. SANOFI reserves the right to refuse such use or reliance on legitimate and reasonable grounds. In any event, subject to Sanofi's prior written agreement, CONTRACTOR shall adhere to the principle of «security by design and by default». The technical, organizational and/or security measures shall be appropriate to the relevant circumstances and the risks, in order to address AI specific vulnerabilities and shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples, adversarial prompting or model inversion attacks, evasion, etc.), confidentiality attacks or model flaws.
CONTRACTOR shall design and implement (a) accuracy tests for AI systems and their outputs, (b) back-up plans to ensure AI systems are resilient to errors and faults, as well as (c) regular monitoring and testing to reduce the risk of biased outputs.

CONTRACTOR shall also (i) design and develop AI systems to achieve an appropriate level of accuracy, robustness, and cybersecurity and (ii) put in place all controls and technical and organizational measures to ensure consistent performance throughout the AI systems lifecycle. CONTRACTOR must declare the levels of accuracy and the relevant accuracy metrics of AI systems in the accompanying instructions for use.

AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce the risk of biased outputs influencing future operations (feedback loops). CONTRACTOR must ensure that any such feedback loops are addressed with appropriate mitigation measures.

AI Usage Policy. The Contractor shall implement regular training programs for employees and other persons dealing with the operation and use of AI systems on its behalf, including:

- The risks associated with the use of unvalidated or insecure AI models and systems (Shadow-AI);
- Recognizing signs of AI misuse;
- Internal AI management policies and compliance with applicable laws, including Security Laws;
- Document and provide proof of participation in training for of the individuals concerned by these trainings.

Implementation of technical measures on proxies or network equipment, such as:

- Filtering connections to limit access to clearly prohibited AI services;
- Regular audit of connection logs to detect non-compliant usage;
- Use of operational solutions to strengthen controls on uses (no logging on platforms, blocking of file uploads, etc.).