МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КАЧЕСТВА	INFORMATION SECURITY AND QUALITY ASSURANCE MEASURES

Меры по обеспечению информационной безопасности и качества, перечисленные в настоящем документе, являются минимальными мерами, которые следует применять в зависимости от характера, контекста и объема услуг (далее — **«Меры по обеспечению информационной безопасности и качества»**). Подтверждение таких мер САНОФИ (при наличии) не освобождает ПОСТАВЩИКА от его обязательств по настоящему документу и любому соглашению, включая договор присоединения, заключенному между САНОФИ и ПОСТАВЩИКОМ (далее — **«Соглашение»**) (в зависимости от обстоятельств).

The information security and quality assurance measures listed in this document are the minimum measures to be applied depending on the nature, context and scope of the services (hereinafter referred to as **"Information Security and Quality Assurance Measures"**). Confirmation of such measures by SANOFI, if any, shall not relieve the SUPPLIER of its obligations hereunder or under any agreement, including the accession contract, between SANOFI and the SUPPLIER (hereinafter referred to as the **"Contract"**) (as the case may be).

ПОСТАВЩИК обязуется за свой счет обеспечить соблюдение всех Мер по обеспечению информационной безопасности и качества, перечисленных в настоящем документе.

The SUPPLIER shall at its own cost ensure that all Information Security and Quality Assurance Measures listed in this document are complied with.

Если ПОСТАВЩИК считает, что какая-либо Мера по обеспечению информационной безопасности и качества неприменима в силу характера, контекста и объема Услуг, он должен подтвердить это письменными доказательствами.

If the SUPPLIER considers that any Information Security and Quality Assurance Measure is not applicable due to the nature, context and scope of the Services, it shall confirm this with written evidence.

Термины, используемые в настоящем документе с заглавной буквы, имеют значения, указанные в Соглашении, если иное не определено в настоящем документе.

Capitalized terms used herein will have the meanings given to them in the Contract unless otherwise defined herein.

ОПРЕДЕЛЕНИЯ

DEFINITIONS

Аффилированная (-ые) компания (-и) — в зависимости от того, что применимо в отношении САНОФИ или ПОСТАВЩИКА, любая компания, которая прямо или косвенно контролируется компанией «Санофи» (зарегистрированной в Париже, номер в торговом реестре: 395 030 844) или ПОСТАВЩИКОМ или находится под ее или его общим контролем.

Affiliate(s): whichever is applicable to SANOFI or SUPPLIER, any company that is directly or indirectly controlled by Sanofi (registered in Paris, trade register number: 395 030 844) or the SUPPLIER or is under its or its common control.

Применимое законодательство — все законы, правила (включая применимый закон о защите данных), применимый кодекс поведения, политика и лицензии регуляторных органов, включая, помимо прочего, нормативные положения и (или) кодекс поведения для предприятий фармацевтической промышленности, закон об обеспечении конфиденциальности, трудовое законодательство, законодательство о защите данных, правила в области охраны труда, техники

Applicable Laws: all laws, regulations (including applicable data protection law), applicable code of conduct, policies and licenses of regulatory authorities, including, without limitation, regulations and/or code of conduct for the pharmaceutical industry, privacy law, labor law, data protection law, health, safety and environmental regulations in force during the term of the Contract in the relevant territory, including any amendments to any regulations relevant to the subject

безопасности и охраны окружающей среды, действующие в течение срока действия Соглашения на соответствующей территории, включая любые поправки к любым нормативным актам, имеющим отношение к предмету Соглашения. Применимое законодательство включает надлежащую лабораторную практику, надлежащую клиническую практику, надлежащую отраслевую практику и (или) надлежащую производственную практику (**GxP**).

matter of the Contract. Applicable Law includes Good Laboratory Practice, Good Clinical Practice, Good Industry Practice and/or Good Manufacturing Practice (**GxP**).

Применимый закон о защите данных — законы, правила и нормативные положения о защите персональных данных, применимые в стране учреждения Контролера данных. В частности, на любую обработку данных распространяется Общий регламент о защите персональных данных (GDPR) (в рамках его применения к данному виду обработки), а также любые дополнительные нормативные положения и правила, действующие в соответствующей стране-члене Европейского союза, применимые к обработке данных.

Applicable Data Protection Law: the laws, rules and regulations on the protection of personal data applicable in the country of the establishment of the Data Controller. In particular, any data processing is subject to the General Data Protection Regulation (GDPR) (as it applies to that type of processing), as well as any additional regulations and rules in force in the relevant European Union member state applicable to the data processing.

Журнал (-ы) контроля — хронологическая запись событий, таких как создание, изменение, удаление записи или электронной записи (по GxP или не по GxP) и возможность получения доступа к ней, которая позволяет реконструировать ход событий и содержит данные о тех, кто ее создал, получал к ней доступ, изменил или удалил ее и причинах их действий.

Audit Trail(s): A historical record of events, such as the creation, modification, deletion of a record or electronic record (GxP or non-GxP) and the ability to access it, that allows you to reconstruct the course of events and contains information about who created it, accessed it, modified or deleted it, and the reasons for their actions.

Данные клиента — любые данные, информация, текст, рисунки, изображения, видео, звуки, статистика, анализ и другие материалы, содержащиеся в любой форме, относящиеся к САНОФИ или его Аффилированным компаниям и (или) пользователям (в соответствующих случаях), которые могли быть предоставлены САНОФИ или его Аффилированными компаниями (и (или) его пользователями) (включая Персональные данные) и (или) к которым ПОСТАВЩИК имеет доступ, и (или) которые ПОСТАВЩИК создает, собирает, обрабатывает, хранит или передает в ходе выполнения Соглашения и связанный с такими данными Журнал контроля.

Customer Data: means any data, information, text, drawings, images, videos, sounds, statistics, analysis and other materials contained in any form relating to SANOFI or its Affiliates and/or users (as applicable) that may have been provided by SANOFI or its Affiliates (and/or its users) (including Personal Data) and/or to which the SUPPLIER has access, and/or which the SUPPLIER creates, collects, processes, stores or transfers in the course of the execution of the Contract and the Audit Trail associated with such data.

Среда Клиента — имеющаяся в настоящее время компьютерная и телекоммуникационная среда САНОФИ (состоящая из аппаратного и программного обеспечения), указанная в Соглашении или обозначенная САНОФИ для ПОСТАВЩИКА как среда для предоставления Услуг.

Client Environment: SANOFI's currently available computer and telecommunication environment (consisting of hardware and software) specified in the Contract or designated by SANOFI to the SUPPLIER as an environment for the provision of the Services.

Контроль — прямое или косвенное владение не менее чем 50 % (пятьюдесятью процентами) акционерного капитала или более чем 50 % (пятьюдесятью процентами) прав голоса или наличие полномочий для назначения большинства членов своего основного

Control: the direct or indirect ownership of at least fifty per cent (50%) of the share capital, or more than fifty per cent (50%) of the voting rights, or the power to appoint a majority of the members of its principal governing body.

органа управления.

Термин «Контролер» употребляется в значении, указанном в GDPR.

The term "Controller" has the meaning given to it in the GDPR.

Целостность данных — характеристика сбора данных в части применения эффективных организационных, операционных и технических средств для обеспечения надежности, конфиденциальности и доступности данных.

Data Integrity: the characteristic of data collection in terms of the use of effective organizational, operational and technical means to ensure the reliability, confidentiality and accessibility of data.

Оборудование — любое оборудование, терминалы, инфраструктура, соответствующее аппаратное и программное обеспечение, включая, где это применимо, системы (то есть все без исключения ИТ-сети или ресурсы, которые обрабатывают, хранят, поддерживают, передают или содержат Данные Клиента), приложения, базы данных, центральный процессор, персональные компьютеры и другие процессоры, контроллеры, устройства хранения, принтеры, телефоны, другие периферийные устройства и устройства ввода и вывода, а также другое физическое механическое и электронное оборудование, предназначенное для обработки, ввода, вывода, хранения и поиска информации и Данных Клиента, а также для работы с ними.

Equipment: means any equipment, terminals, infrastructure, related hardware and software, including, where applicable, systems (i.e., all without exception IT networks or resources that process, store, support, transmit or contain Client Data), applications, databases, central processor, personal computers and other processors, controllers, storage devices, printers, telephones, other peripheral devices and input and output devices, and other physical, mechanical and electronic equipment designed for processing, inputting, outputting, storing, retrieving and handling Client Information and Data as well as for working with it.

GDPR — Регламент (ЕС) 2016/679 Европейского парламента и Совета ЕС от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС.

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

GxP и другие нормативные требования, связанные со сферой здравоохранения — такие нормативные требования, как надлежащая клиническая практика, надлежащая лабораторная практика, надлежащая практика фармаконадзора, надлежащая практика производства и надлежащая практика дистрибуции, а также любые другие нормативные акты, применимые к САНОФИ и относящиеся к сфере общественного здравоохранения.

GxP and other health-related regulatory requirements: such regulatory requirements as Good Clinical Practice, Good Laboratory Practice, Good Pharmacovigilance Practice, Good Manufacturing Practice and Good Distribution Practice, and any other regulations applicable to SANOFI and relating to public health.

Компьютеризированная система GxP — компьютеризированная система, используемая для поддержки надлежащих практик GxP или другой регуляторной деятельности, связанной со сферой здравоохранения.

GxP Computerized System: the computerized system used to support Good Practices (GxP) or other health related regulatory activities.

Инцидент — любое событие, которое не соответствует нормальному процессу и которое может привести к прекращению оказания или снижению качества Услуг, предоставляемых САНОФИ.

Incident: any event that does not correspond to the normal process and that may lead to the termination of the provision or deterioration of the quality of the Services provided to SANOFI.

ИТ-изменение (-я) — любое фактическое или предлагаемое изменение характера, уровня и

IT change(s): any actual or proposed change in the nature, level, scale and/or scope of an IT system.

масштаба и (или) области применения ИТ-системы.

Персонал — (в отношении ПОСТАВЩИКА) (i) любой сотрудник ПОСТАВЩИКА; (ii) любой индивидуальный консультант, действующий под свою ответственность; или (iii) любой поставщик, уполномоченный агент или субподрядчик (включая Аффилированные компании ПОСТАВЩИКА), назначенный для оказания Услуг; (в отношении САНОФИ) (i) любой сотрудник САНОФИ или его Аффилированных компаний; (ii) любой работник агентства; и (или) (iii) любой индивидуальный консультант, действующий под ответственность САНОФИ или его Аффилированных компаний.

Personnel: (with respect to the SUPPLIER) (i) any employee of the SUPPLIER; (ii) any individual consultant acting under its own responsibility; or (iii) any supplier, authorized agent or subcontractor (including the SUPPLIER Affiliates) appointed to perform the Services; (with respect to SANOFI) (i) any employee of SANOFI or its Affiliates; (ii) any agency employee; and/or (iii) any individual consultant acting under the responsibility of SANOFI or its Affiliates.

Персональные данные и обработка — см. определение в GDPR.

Personal Data and Processing: See the definition in the GDPR.

Профессиональные стандарты — в отношении любого конкретного мероприятия или задачи, включенной, рассматриваемой или предусмотренной для выполнения Соглашения: такие стандарты, практики, методы и процедуры, которые соответствуют всем требованиям Применимого законодательства и должны соблюдаться и выполняться с максимальным уровнем квалификации, осмотрительности, внимательности и дальновидности, которого можно обоснованно ожидать от поставщика услуг, осуществляющего аналогичные действия или действующего в аналогичных обстоятельствах, при соответствии с признанными международными стандартами.

Professional Standards: in relation to any particular activity or task included in, contemplated by or contemplated for the performance of the Contract: such standards, practices, methods and procedures as are consistent with all requirements of Applicable Law and shall be followed and performed with the highest level of skill, care, diligence and foresight reasonably expected from a service provider performing similar acts or acting in similar circumstances in accordance with recognized international standards.

Инцидент (-ы) в системе безопасности включает (-ют) в себя, как далее определено в настоящем документе, любой вирус и, помимо прочего, случаи фактического, возможного, предпринятого или угрожающего несанкционированного (i) воздействия, доступа, использования, удаления, доработки, шифрования, воспроизведения, уничтожения, утраты, кражи, изменения, раскрытия, копирования, модификации или передачи любого компонента Данных Клиента, включая конфиденциальную информацию пользователей, который находится или должен находиться под контролем ПОСТАВЩИКА или за которые ПОСТАВЩИК несет ответственность; или, в случае соответствующей ситуации; ii) (физического или иного) доступа, кражи или повреждения любого Оборудования Клиента, которое контролируется ПОСТАВЩИКОМ или для ПОСТАВЩИКА или на котором обрабатываются или хранятся Данные Клиента.

Security Incident (s): shall include, as further defined herein, any virus and, without limitation, any actual, potential, undertaken or threatened unauthorized (i) exposure to, access, use, deletion, modification, encryption, reproduction, destruction, loss, theft, modification, disclosure, copying, modification or transmission of any Client Data component, including user confidential information, that is or should be under the control of, or for which the SUPPLIER is responsible; or, where applicable; (ii) (physical or otherwise) access to, theft of, or damage to, any Client Equipment that is controlled by or for the SUPPLIER, or on which Client Data is processed or stored.

Услуги — услуги, предоставляемые ПОСТАВЩИКОМ САНОФИ.

Services: the services to be delivered to SANOFI by the SUPPLIER.

Закон Сарбейнза–Оксли — Закон Сарбейнза–Оксли от

The Sarbanes-Oxley Act: the Sarbanes-Oxley Act of 2002,

2002 года, также известный как «Закон о реформе бухгалтерского учета в публичных компаниях и защите инвесторов» (в Сенате) и «Закон о корпоративной и аудиторской отчетности, ответственности и прозрачности» (в Палате представителей); часто называемый как SOX (Sarbanes-Oxley Act), — это федеральный закон Соединенных Штатов, который устанавливает новые или расширенные требования для всех американских компаний, управляющих и бухгалтерских фирм.

also known as the Public Company Accounting Reform and Investor Protection Act (in the Senate) and the Corporate and Auditing Accountability, Responsibility, and Transparency Act (in the House of Representatives); often referred to as the SOX (Sarbanes-Oxley Act), is a United States federal law that imposes new or expanded requirements on all American companies, managers, and accounting firms.

Третья (-ьи) сторона (-ы) — любое физическое или юридическое лицо, не являющееся Стороной Соглашения (включая государственные или связанные с ними органы, организации или суды).

Third Party(ies): any person or entity not a Party to the Contract (including governmental or related authorities, organizations, or courts).

1. Обязанности и обязательства в области информационной безопасности

1. Responsibilities and obligations in the field of information security

1.1 Контактные лица по вопросам информационной безопасности и качества

1.1 Contact points for information security and quality issues

ПОСТАВЩИК обязан назначить лицо, ответственное за информационную безопасность. Такое лицо будет считаться единственным контактным лицом по вопросам информационной безопасности и будет отвечать за реализацию всех Мер по обеспечению информационной безопасности и качества, перечисленных в настоящем документе.

The SUPPLIER is obliged to appoint a person responsible for information security. Such a person will be considered the sole point of contact for information security issues and will be responsible for the implementation of all Information Security and Quality Assurance Measures listed in this document.

Лицо, ответственное за информационную безопасность, должно назначить себе заместителя на случай своего отсутствия.

The person responsible for information security must appoint a deputy in case of absence.

ПОСТАВЩИК обязан назначить лицо, ответственное за качество (в контексте применения GxP и других правил, связанных со сферой здравоохранения). Такое лицо будет считаться единственным контактным лицом по вопросам качества и будет отвечать за реализацию всех Мер по обеспечению информационной безопасности и качества, перечисленных в настоящем документе.

The SUPPLIER is obliged to appoint a person responsible for quality (in the context of the application of GxP and other rules related to the field of health care). Such a person will be considered the sole point of contact for quality issues and will be responsible for the implementation of all Information Security and Quality Assurance Measures listed in this document.

Лицо, ответственное за качество, должно назначить себе заместителя на случай своего отсутствия.

The person responsible for quality must appoint a deputy in case of absence.

1.2 Программа обеспечения информационной безопасности

1.2 Information Security Program

ПОСТАВЩИК должен разработать, контролировать, а также, при необходимости, дорабатывать и актуализировать содержание комплексной Программы обеспечения информационной безопасности (в письменном виде), применяемой к облаку и (или) Услугам, а также к защите безопасности и целостности данных.

The SUPPLIER shall develop, monitor, and, if necessary, finalize and update the content of a comprehensive Information Security Program (in writing) applicable to the cloud and/or Services, as well as to data security and integrity protection.

Такая Программа обеспечения информационной

Such Information Security Program shall comply with

безопасности должна соответствовать Профессиональным стандартам и содержать задокументированные политики и процедуры, а также административные, технические и физические меры обеспечения безопасности для защиты безопасности, целостности и конфиденциальности облака, Услуг и Данных клиентов.

Professional Standards and shall contain documented policies and procedures and administrative, technical and physical security measures to protect the security, integrity and confidentiality of the Cloud, Services and Client Data.

1.3 План обеспечения безопасности

ПОСТАВЩИК должен разработать, контролировать, а также, при необходимости, дорабатывать и актуализировать содержание комплексного плана обеспечения безопасности (**План обеспечения безопасности** в письменном виде). План обеспечения безопасности должен описывать способ реализации ПОСТАВЩИКОМ, если это применимо, каждой меры обеспечения безопасности, перечисленной в настоящем документе. План обеспечения безопасности должен быть утвержден САНОФИ до начала оказания Услуг.

1.3 Safety Management Plan

The SUPPLIER shall develop, monitor and, if necessary, finalize and update the contents of the integrated security plan (written **security plan**). The security plan shall describe how the SUPPLIER will implement, if applicable, each security measure listed in this document. The security plan must be approved by SANOFI prior to the commencement of the Services.

1.4 Программа оценки рисков

ПОСТАВЩИК должен обеспечивать и осуществлять регулярную оценку внутренних и внешних рисков для безопасности, конфиденциальности, целостности и доступности Данных Клиента, включая, помимо прочего, выявление и оценку уязвимостей для Оборудования ПОСТАВЩИКА.

1.4 Risk Assessment Program

The SUPPLIER shall ensure and regularly assess the internal and external risks to the security, confidentiality, integrity and availability of the Client Data, including, but not limited to, the identification and assessment of vulnerabilities to the SUPPLIER’s Equipment.

1.5 Политика допустимого использования

ПОСТАВЩИК должен утвердить политику допустимого использования, с которой должен быть ознакомлен его Персонал до получения любого доступа к Оборудованию ПОСТАВЩИКА.

1.5 Acceptable use policy

The SUPPLIER shall approve the Acceptable Use Policy, which shall be communicated to its Personnel prior to any access to the SUPPLIER’s Equipment.

1.6 Расследования в области безопасности

ПОСТАВЩИК должен в полной мере сотрудничать с САНОФИ в случае проведения любого расследования в области безопасности по возможным нарушениям его обязательств в отношении информационной безопасности.

1.6 Security Investigations

The SUPPLIER shall cooperate fully with SANOFI in the event of any security investigation of possible breaches of its information security obligations.

1.7 Уведомление о проблемах безопасности

ПОСТАВЩИК должен сообщать САНОФИ и уведомлять его в течение 24 (двадцати четырех) часов о любой потенциальной проблеме в области безопасности, возникшей в отношении Оборудования, решений или данных ПОСТАВЩИКА и (или) САНОФИ, или о любом другом событии, информация о котором должна быть предоставлена в соответствии с Применимым законодательством. ПОСТАВЩИК не должен использовать такие проблемы в области безопасности или раскрывать информацию о них и

1.7 Security Problem Notification

The SUPPLIER shall report to and notify SANOFI, within twenty-four (24) hours, of any potential security issue arising with respect to the SUPPLIER’s Equipment, solutions or data and/or SANOFI or any other event to be reported in accordance with the Applicable Laws. The SUPPLIER shall not use or disclose such security concerns and shall correct them as soon as reasonably practicable and under any circumstances before they give rise to a Security Incident.

обязан устранить их в кратчайшие сроки и при любых обстоятельствах до того, как они приведут к Инциденту в системе безопасности.

1.8 Управление инцидентами в области безопасности

ПОСТАВЩИК обязан осуществлять управление такими инцидентами и приступать к минимизации последствий инцидентов в системе безопасности в отношении оборудования и (или) услуг, предоставляемых САНОФИ ПОСТАВЩИКОМ, выполняя процедуру управления инцидентами и план надлежащего реагирования.

1.8 Security Incident Management

The SUPPLIER shall manage such incidents and proceed to minimize the consequences of security incidents with respect to the equipment and/or services provided by the SUPPLIER to SANOFI, following an incident management procedure and an appropriate response plan.

1.9 Управление изменениями

ПОСТАВЩИК должен следовать формальному процессу управления ИТ-изменениями для контроля любых ИТ-изменений, которые потенциально могут повлиять на целостность данных САНОФИ, соответствие требованиям, функциональность или доступность Услуг, предоставляемых САНОФИ. ПОСТАВЩИК обязан вносить ИТ-изменения в Данные Клиента, используя обычные функциональные возможности Услуг.

1.9 Change management

The SUPPLIER shall follow a formal IT change management process to control any IT changes that have the potential to impact SANOFI's data integrity, compliance, functionality or availability of the Services provided by SANOFI. The SUPPLIER shall make IT changes to Client Data using the normal functionality of the Services.

ПОСТАВЩИК должен предоставить САНОФИ специальную предварительную среду для проведения надлежащего тестирования ИТ-изменений перед их внедрением в рабочую среду.

The SUPPLIER must provide SANOFI with a special preliminary environment for proper testing of IT changes before they are introduced into the working environment.

ПОСТАВЩИК обязуется предоставить САНОФИ уведомление за 30 (тридцать) дней до внесения любых ИТ-изменений, которые прямо или косвенно влияют на Услуги. Регулярные операции, такие как техническое обслуживание или реагирование на Инциденты, не считаются ИТ-изменениями и должны осуществляться в рамках установленных процессов.

The SUPPLIER must provide SANOFI with thirty (30) days prior to notice of any IT changes that directly or indirectly affect the Services. Regular operations such as maintenance or incident response are not considered IT changes and must be carried out within the established processes.

В случае сбоев или проблем, возникающих в результате внесения ИТ-изменений, ПОСТАВЩИК должен иметь возможность вернуться к исходному состоянию, чтобы вернуть Услуги, которые используются САНОФИ или для него, или Данные Клиента в состояние до момента реализации ИТ-изменения.

In the event of disruptions or problems arising from an IT change, the SUPPLIER shall be able to return to its original state in order to return the Services used by or for SANOFI or the Client Data to a state prior to the implementation of the IT change.

2. <u>Безопасность инфраструктуры</u>

2. <u>Infrastructure Safety</u>

2.1 Сетевая безопасность

2.1 Network security

ПОСТАВЩИК обязан применять Профессиональные стандарты при разделении сети, включая, помимо прочего, следующие меры:

- каждая сеть должна быть изолирована от других сетей с помощью брандмауэров или аналогичных мер;

The SUPPLIER is obliged to apply the Professional Standards in the separation of the network, including, but not limited to, the following measures:

- each network shall be isolated from other networks by means of firewalls or equivalent measures;

- должны быть разрешены только утвержденные входящие и (или) исходящие коммуникационные потоки.

- only approved incoming and/or outgoing communication flows shall be allowed.

2.2 Защита сетевых протоколов

ПОСТАВЩИК должен обеспечить безопасность и актуальность всех сетевых протоколов и отсутствие в них известных уязвимостей.

2.2 Protection of network protocols

The SUPPLIER shall ensure that all network protocols are secure, up-to-date and free of known vulnerabilities.

2.3 Усиление инфраструктуры

ПОСТАВЩИК должен обеспечить усиление ключевых компонентов своей сети, сетевых потоков и операционных систем, а также максимальное ограничение видов атак. К этим мерам могут относиться, помимо прочего, следующие:

- фильтрация сетевых потоков, отключение неиспользуемых или устаревших сетевых протоколов;
- деактивация неиспользуемых или устаревших сервисов или функций операционных систем;
- отключение неиспользуемых или устаревших служб, функций или физических портов сетевого оборудования;
- изменение паролей по умолчанию, используемых для администрирования и (или) подключения;
- строгий контроль за установкой программного обеспечения и (или) надстроек;
- строгий контроль за изменением конфигурации.

2.3 Reinforce the infrastructure

The SUPPLIER shall ensure that the key components of its network, network flows and operating systems are enhanced, and that the types of attacks are limited as much as possible. These measures may include, but are not limited to, the following:

- filtering network streams, disabling unused or outdated network protocols;
- deactivation of unused or outdated services or functions of operating systems.
- disabling unused or outdated services, functions or physical ports of the network equipment;
- changing the default passwords used for administration and/or connection;
- strict control over the installation of software and/or add-ons;
- strict control over configuration changes.

2.4 Защита от вредоносных программ

ПОСТАВЩИК обязуется обеспечить защиту ключевых компонентов сети и Оборудования от всех типов известных вредоносных программ с помощью достаточных и актуальных средств защиты от вредоносных программ.

2.4 Protection from malware

The SUPPLIER undertakes to protect the key components of the network and the Equipment from all types of known malware with sufficient and up-to-date malware protection.

2.5 Документация сети

ПОСТАВЩИК должен обеспечить наличие документации по своей сетевой архитектуре.

2.5 Network Documentation

The SUPPLIER shall maintain documentation for its network architecture.

2.6 Защита платформ администрирования

ПОСТАВЩИК должен ограничить любые платформы и инфраструктуру удаленного администрирования IP-адресами источников ПОСТАВЩИКА.

2.6 Protection of administration platforms

The SUPPLIER shall restrict any remote administration platforms and infrastructure to the pool of IP addresses for the SUPPLIER's sources.

2.7 Защита беспроводных сетей

ПОСТАВЩИК должен обеспечить надлежащую защиту своих беспроводных сетей. Для этого могут быть реализованы следующие меры (список может

2.7 Wireless Network Security

The SUPPLIER shall ensure that its wireless networks are adequately protected. To do this, the following measures

быть расширен):

- защита беспроводного доступа безопасным протоколом аутентификации и ключом достаточной длины;
- мощность точек беспроводного доступа должна соответствовать занимаемой ПОСТАВЩИКОМ территории, чтобы гарантировать невозможность доступа к беспроводной сети за пределами территории ПОСТАВЩИКА (за пределами зданий);
- изменение установленных по умолчанию учетных данных и (или) паролей для подключения к точкам беспроводного доступа;
- отключение неиспользуемых или устаревших услуг, протоколов, функций или физических портов для беспроводного доступа;
- обновление прошивки беспроводных сетевых устройств;
- проверка подлинности и авторизация для всех беспроводных подключений.

2.8 Специализированные сервисы и среда внешнего размещения

Среда обработки услуг САНОФИ должна быть логически отделена от других клиентов ПОСТАВЩИКА с помощью выделенного отдельного сервера. Данные Клиента должны физически находиться в выделенной среде базы данных в выделенном экземпляре базы данных.

2.9 Защита мобильных устройств

Если Персонал ПОСТАВЩИКА использует собственные и (или) корпоративные мобильные устройства для оказания Услуг САНОФИ:

- ПОСТАВЩИК обязан защищать свои мобильные устройства паролем. Такой пароль должен соответствовать следующим правилам:
  - длина пароля: минимум 8 символов;
  - блокировка пароля по времени: пароль необходимо повторно ввести через 5 минут бездействия;
  - смена пароля: пароль необходимо менять ежегодно;
  - история паролей: последние два пароля не должны использоваться повторно.
- ПОСТАВЩИК обязан управлять мобильными устройствами своего персонала и осуществлять их администрирование.
- ПОСТАВЩИК обязан обеспечить четкое разделение между профессиональными и частными приложениями и данными.
- Если какие-либо Данные Клиента хранятся на каком-либо мобильном устройстве, такие

can be implemented (the list can be extended):

- secure wireless access with a secure authentication protocol and a key of sufficient length;
- the capacity of the wireless access points must correspond to the territory occupied by the SUPPLIER in order to guarantee the inability to access the wireless network outside the SUPPLIER's territory (outside the buildings);
- changing default credentials and/or passwords for connecting to wireless access points.
- disabling unused or outdated services, protocols, functions, or physical ports for wireless access.
- updating the firmware of wireless network devices;
- authentication and authorization for all wireless connections.

2.8 Specialized services and external hosting environment

The SANOFI Service Processing Environment shall be logically segregated from other SUPPLIER's clients by a dedicated separate server. Client Data must be physically located in a dedicated database environment in a dedicated database instance.

2.9 Mobile device protection

If SUPPLIER Personnel use their own and/or corporate mobile devices to provide SANOFI Services:

- The SUPPLIER shall protect its mobile devices with a password. Such a password should adhere to the following rules:
  - password length: at least 8 characters;
  - time password lock: the password must be re-entered after 5 minutes of inactivity;
  - password change: the password must be changed annually;
  - password history: the last two passwords should not be reused.
- The SUPPLIER shall manage and administer the mobile devices of its personnel.
- The SUPPLIER shall ensure a clear separation between professional and private applications and data.
- If any Client Data is stored on any mobile device,

данные должны быть в зашифрованном виде.

such data shall be encrypted.

2.10 Программа управления оборудованием

ПОСТАВЩИК обязан использовать передовой опыт управления оборудованием и ИТ-инфраструктурой в отношении собственного Оборудования и Оборудования, управляемого САНОФИ (управление сетью, оконечными устройствами, идентификацией и доступом пользователей) (корректировка и регулярное обновление, прогнозирование устаревания).

2.10 Equipment control program

The SUPPLIER shall use the best practices of equipment and IT infrastructure management with respect to its own Equipment and SANOFI-Managed Equipment (management of network, terminal devices, user identification and access) (correction and regular updating, forecasting of obsolescence).

2.11 Договоры на техническое обслуживание

ПОСТАВЩИК обязан иметь в наличии договоры на техническое обслуживание с точки зрения информационной безопасности со всеми поставщиками Оборудования.

2.11 Maintenance contracts

The SUPPLIER shall have information security maintenance contracts with all suppliers of the Equipment.

2.12 Безопасность удаленной работы

ПОСТАВЩИК обязан иметь в наличии политику организации удаленной работы, которая эффективно защищает Данные Клиента и Оборудование. По запросу САНОФИ ему может быть предоставлена информация о такой политике.

2.12 Security for remote work

The SUPPLIER shall have a remote work organization policy that effectively protects the Client Data and the Equipment. At SANOFI's request, the SUPPLIER may be provided with information on such policies.

3. <u>Удаленный доступ</u>

3. <u>Remote Assistance</u>

3.1 Контроль доступа

ПОСТАВЩИК обязан документировать свои процедуры удаленного доступа. Удаленный доступ должен основываться на защищенных сетевых протоколах и использовать двухфакторную проверку подлинности.

3.1 Access control

The SUPPLIER shall document its remote access procedures. Remote access should be based on secure network protocols and use two-factor authentication.

3.2 Защита паролей

С целью надежного управления паролями ПОСТАВЩИК должен обеспечить соответствие своей политики в отношении паролей передовым отраслевым стандартам (Password Protection Policy («Политика защиты паролей») от Института SANS или DAT-NT-001/ANSSI/SDE/NP от агентства ANSSI), которые включают, помимо прочего, следующие минимальные требования):

- минимальная длина пароля: минимум 8 символов;
- сложность пароля: 3 различных типа символов, включая прописные буквы, строчные буквы, цифры и специальные символы;
- смена пароля:пароль необходимо менять каждые 3 месяца;
- ограничение возможности повторного

3.2 Password protection

For the purpose of secure password management, the SUPPLIER shall ensure that its password policy complies with industry-leading standards (Password Protection Policy from SANS Institute or DAT-NT-001/ANSSI/SDE/NP from ANSSI), which include, but are not limited to, the following minimum requirements:

- minimum password length: minimum 8 characters.
- password complexity: 3 different types of characters, including uppercase letters, lowercase letters, numbers and special characters;
- change of password:the password must be changed every 3 months;
- restrict the ability to reuse passwords (at least after

использования паролей (минимум после 10 замен);
- блокировка учетной записи через 5 минут бездействия.

10 changes).
- account lockout after 5 minutes of inactivity.

ПОСТАВЩИК обязан обеспечить шифрование паролей во время передачи и изменение паролей при первом подключении.

The SUPPLIER is obliged to ensure password encryption during transmission and password change at the first connection.

ПОСТАВЩИК обязан предпринимать меры, запрещающие его Персоналу хранить и записывать пароли в открытом виде.

The SUPPLIER shall take measures to prohibit its Personnel from storing and recording passwords openly.

3.3 Физический доступ к Среде Клиента

Если ПОСТАВЩИКУ необходимо получить доступ к интернету во время нахождения на территории САНОФИ, ПОСТАВЩИК должен воздержаться от использования локальной сети САНОФИ, если САНОФИ не предоставит соответствующее оборудование. Если такое оборудование не будет предоставлено САНОФИ, ПОСТАВЩИКУ строго запрещено использование локальной сети САНОФИ, но он может использовать гостевую сеть Wi-Fi, запросив код доступа у САНОФИ.

3.3 Physical access to the Client Environment

If the SUPPLIER needs to access the Internet while in SANOFI territory, the SUPPLIER shall refrain from using the SANOFI LAN if SANOFI does not provide the relevant equipment. If such equipment is not provided by SANOFI, the SUPPLIER is strictly prohibited from using the SANOFI LAN, but can use the Wi-Fi guest network by requesting an access code from SANOFI.

3.4 Контроль физического доступа к Данным Клиента

ПОСТАВЩИК обязан применять и поддерживать обоснованные ограничения на физический доступ к Данным Клиента, включая процедуру, устанавливающую способ ограничения физического доступа.

3.4 Physical Access Controls to Client Data

The SUPPLIER shall apply and maintain reasonable restrictions on physical access to Client Data, including a procedure establishing how to restrict physical access.

ПОСТАВЩИК обязан вести журнал контроля любого физического доступа к местам размещения Данных Клиента.

The SUPPLIER shall maintain a log of any physical access to Client Data locations.

3.5 Контроль логического доступа к Данным Клиента

Если ПОСТАВЩИК размещает, обрабатывает, передает или собирает Данные Клиента:
- ПОСТАВЩИК обязан документировать, внедрять, поддерживать и обновлять надлежащие меры обеспечения безопасности, которые гарантируют, что ПОСТАВЩИК будет использовать Данные Клиента или получать доступ к Данным Клиента исключительно по прямому запросу САНОФИ или с его одобрения, а также при наличии обоснованной установленной деловой потребности, подтвержденной САНОФИ;
- учетные данные для логического доступа к Данным Клиента должны быть строго ограничены уполномоченным персоналом ПОСТАВЩИКА;

3.5 Control of logical access to Client Data

If the SUPPLIER places, processes, transfers, or collects Client Data:
- The SUPPLIER shall document, implement, maintain and update appropriate security measures that ensure that the SUPPLIER will use Client Data or access Client Data solely upon SANOFI's express request or approval, and if there is a reasonable established business need confirmed by SANOFI;
- the credentials for the logical access to the Client Data shall be strictly limited to the authorized personnel of the SUPPLIER;

- ПОСТАВЩИК обязан вести учет всего авторизованного логического доступа к Данным Клиента.

ПОСТАВЩИК должен вести список своего Персонала, который имел и (или) имеет доступ к Данным Клиента с использованием внешних и внутренних полномочий доступа. ПОСТАВЩИК обязан предоставлять документально подтвержденные доказательства по запросу САНОФИ.

И ПОСТАВЩИК, и САНОФИ должны гарантировать, что (i) только уполномоченный персонал может получить доступ к Услугам и (или) Данным Клиента или использовать их; (ii) ведется учет операций по созданию, изменению и деактивации полномочий пользователей; (iii) пользователи проходят практическое обучение до согласования их запросов на доступ; (iv) уровни полномочий для доступа соответствуют обязанностям и роли в системе.

3.6 Контроль логического доступа к сетям САНОФИ

Если Персонал ПОСТАВЩИКА осуществляет удаленную установку, обслуживание или администрирование какого-либо Оборудования:

- ПОСТАВЩИК обязан документировать, внедрять, поддерживать и обновлять надлежащие меры обеспечения безопасности, которые гарантируют, что его Персонал будет получать доступ к Оборудованию Клиента исключительно по прямому запросу САНОФИ или с его одобрения, а также при наличии обоснованной установленной деловой потребности, подтвержденной САНОФИ.
- Только уполномоченный Персонал ПОСТАВЩИКА должен иметь Коды доступа к сетям САНОФИ.

Для оказания Услуг ПОСТАВЩИКУ может быть предоставлен удаленный доступ к Среде Клиента.

Для предоставления ПОСТАВЩИКУ доступа к Среде Клиента САНОФИ должен предоставить ПОСТАВЩИКУ один или несколько идентификаторов и один или несколько паролей (далее совместно — «**Коды доступа**»). ПОСТАВЩИК должен обращаться с Кодами доступа как со строго конфиденциальной информацией и не должен разглашать или передавать Коды доступа своему Персоналу или третьим лицам.

ПОСТАВЩИК обязан использовать Коды доступа только в целях и в течение срока, необходимого для оказания Услуг, и предпримет все разумные меры,

- The SUPPLIER shall maintain a record of all authorized logical access to Client Data.

The SUPPLIER shall maintain a list of its Personnel who had and/or have access to Client Data using external and internal access authorities. The SUPPLIER shall provide documented evidence as requested by SANOFI.

Both the SUPPLIER and SANOFI shall ensure that (i) only authorized personnel can access or use the Services and/or Client Data; (ii) records are kept of operations to create, modify, and deactivate user permissions; (iii) users receive hands-on training prior to agreeing on their access requests; and (iv) the levels of access permissions are consistent with responsibilities and roles in the system.

3.6 Logical access control to SANOFI networks

If the SUPPLIER Personnel performs remote installation, maintenance or administration of any Equipment:

- The SUPPLIER shall document, implement, maintain, and update appropriate security measures to ensure that its Personnel will only access the Client's Equipment at Sanofi's express request or with SANOFI's approval and if there is a reasonable established business need confirmed by SANOFI.
- Only authorized SUPPLIER Personnel shall have SANOFI Network Access Codes.

For the provision of the Services, the SUPPLIER may be granted remote access to the Client Environment.

In order to provide the SUPPLIER with access to the Client Environment, SANOFI shall provide the SUPPLIER with one or more identifiers and one or more passwords (collectively, "**Access Codes**"). The SUPPLIER shall treat the Access Codes as strictly confidential and shall not disclose or transfer the Access Codes to its Personnel or third parties.

The SUPPLIER shall use the Access Codes only for the purpose and for the period necessary for the performance of the Services and shall take all reasonable steps to warn

чтобы предупредить САНОФИ о любых нарушениях в работе Среды Клиента или ее содержимого.

SANOFI of any irregularities in the Client Environment or its contents.

Если ПОСТАВЩИК будет распространять или использовать эти Коды доступа способом, который считается противоречащим положениям настоящего Соглашения, САНОФИ может по своему усмотрению отозвать Коды доступа, приостановить или расторгнуть настоящее Соглашение по причине несоблюдения его условий.

If the SUPPLIER distributes or uses these Access Codes in a manner deemed to be in conflict with the provisions of this Contract, SANOFI may, in its sole discretion, revoke the Access Codes, suspend or terminate this Contract for failure to comply with its terms.

ПОСТАВЩИК признает, что САНОФИ может контролировать деятельность ПОСТАВЩИКА в Среде Клиента по усмотрению САНОФИ в соответствии с Применимым законодательством, как указано в политике САНОФИ по использованию информационных технологий (ИТ) и решений, которая периодически обновляется, заменяется и (или) дополняется САНОФИ.

The SUPPLIER acknowledges that SANOFI may control the SUPPLIER’s activities in the Client's Environment at SANOFI's discretion in accordance with the Applicable Laws as specified in SANOFI's Information Technology (IT) and Solutions Policy, which is updated, replaced and/or supplemented by SANOFI from time to time.

ПОСТАВЩИК подтверждает получение указанной политики до предоставления какого-либо доступа к объекту и соглашается с условиями такого контроля.

The SUPPLIER shall acknowledge receipt of said policy prior to granting any access to the facility and agrees to the terms of such control.

ПОСТАВЩИК несет единоличную ответственность за использование Кодов доступа Третьими лицами или за их действия с ними (с целью мошенничества или иной целью). ПОСТАВЩИК обязуется ограждать САНОФИ от любых претензий или убытков, связанных с использованием Кодов доступа или использованием Среды Клиента или доступом к ней или возникающих в результате любых действий, совершаемых в Среде Клиента или посредством Среды Клиента с использованием Кодов доступа. Кроме того, САНОФИ не имеет обязательств или технических средств для проверки личности лиц, использующих Коды доступа. Если у ПОСТАВЩИКА есть основания полагать, что его Коды доступа использует постороннее лицо, он должен немедленно сообщить об этом САНОФИ. Все действия, совершенные с помощью Кодов доступа, считаются выполненными ПОСТАВЩИКОМ.

The SUPPLIER shall be solely responsible for the use of the Access Codes by or with Third Parties (for fraudulent or other purposes). The SUPPLIER undertakes to indemnify SANOFI from and against any claim or loss arising out of or in connection with the use of the Access Codes or the use of or access to the Client Environment or arising out of any action taken in or through the Client Environment using the Access Codes. In addition, SANOFI has no obligation or technical means to verify the identity of persons using the Access Codes. If the SUPPLIER has reason to believe that his Access Codes are used by an unauthorized person, he must immediately inform SANOFI. All actions performed using Access Codes shall be deemed to have been performed by the SUPPLIER.

3.7 Контроль физического доступа в помещения САНОФИ

3.7 Controlling physical access to the SANOFI premises

Если управление помещениями САНОФИ передается на аутсорсинг ПОСТАВЩИКУ:

- ПОСТАВЩИК обязан применять и поддерживать обоснованные ограничения на физический доступ к помещениям Клиента, включая процедуру, устанавливающую способ ограничения физического доступа;
- ПОСТАВЩИК обязан вести журнал контроля любого физического доступа в помещения САНОФИ.

If the management of the SANOFI premises is outsourced to the SUPPLIER:

- The SUPPLIER shall apply and maintain reasonable restrictions on physical access to the Client's premises, including a procedure establishing a method of restricting physical access;
- The SUPPLIER shall maintain a logbook to control any physical access to the SANOFI premises.

3.8 Регистрация и контроль доступа

ПОСТАВЩИК должен регистрировать все действия, связанные с доступом к Данным Клиента, включая запросы на доступ. Срок хранения такой информации должен соответствовать местным нормативным актам и согласовываться с САНОФИ.

3.9 Доступ третьих лиц

ПОСТАВЩИК не должен предоставлять никаким Третьим лицам доступ к Данным или Среде Клиента в инфраструктуре ПОСТАВЩИКА или САНОФИ без предварительного письменного разрешения САНОФИ.

3.10 Постоянный доступ к Данным Клиента

ПОСТАВЩИК должен обеспечивать доступ САНОФИ к Данным Клиента на протяжении всего срока оказания Услуг в заранее согласованном с САНОФИ формате.

4. Безопасность приложений

4.1 Интегрирование информационной безопасности в разработку приложений

Если ПОСТАВЩИК считается разработчиком / поставщиком / интегратором приложения, ПОСТАВЩИК обязан обеспечить реализацию следующих мер (помимо прочего):

- ПОСТАВЩИК обязан интегрировать на всех этапах жизненного цикла разработки приложения требования, касающиеся информационной безопасности приложения с точки зрения конфиденциальности, целостности, доступности и отслеживаемости;
- ПОСТАВЩИК обязан полагаться на передовой опыт Открытого проекта обеспечения безопасности веб-приложений (OWASP) в области защищенной разработки приложений;
- ПОСТАВЩИК обязан отделить среду (среды) разработки приложений от среды (сред) производства приложений;
- ПОСТАВЩИК обязан обеспечить доступ к среде разработки и производства с учетом передового опыта и обеспечить разделение обязанностей;
- ПОСТАВЩИК обязан обеспечить (i) анализ и оценку исходного кода приложения на предмет наличия в нем опубликованных хорошо известных уязвимостей в исходном коде с точки зрения информационной безопасности; и (ii) отсутствие кода, предназначенного для повреждения данных

3.8 Registration and Access Controls

The SUPPLIER shall record all actions associated with the access to the Client Data, including requests for access. The period of storage of such information must comply with local regulations and be agreed with SANOFI.

3.9 Third party access

The SUPPLIER shall not grant access to the Client Data or Environment in the SUPPLIER's or SANOFI's infrastructure to any Third Party without the prior written permission of SANOFI.

3.10 Uninterrupted Access to Client Data

The SUPPLIER shall provide SANOFI with access to Client Data for the duration of the Services in the format previously agreed with SANOFI.

4. Application Security

4.1 Integration of information security into application development

If the SUPPLIER is considered to be the developer/supplier/integrator of the application, the SUPPLIER shall ensure that the following measures are implemented (among others):

- The SUPPLIER is obliged to integrate at all stages of the application development life cycle the requirements related to the application information security in terms of confidentiality, integrity, availability and traceability;
- The SUPPLIER is obliged to rely on the best practices of the Open Web Application Security Project (OWASP) in the field of secure application development;
- The SUPPLIER shall separate the application development environment(s) from the application production environment(s);
- The SUPPLIER shall ensure access to the development and production environment taking into account the best practices and ensure the division of responsibilities;
- The SUPPLIER shall ensure that it (i) analyzes and evaluates the source code of the application for the presence of published well-known vulnerabilities in the source code from an information security perspective; and (ii) there is no code designed to damage data or adversely affect the performance of computer systems

или неблагоприятного воздействия на производительность компьютерных систем (включая любые вирусы, черви, «логические бомбы», отключающие коды, бэкдоры, подпрограммы или сроки действия). ПОСТАВЩИК должен предоставить САНОФИ по его запросу любые доказательства проведенного анализа;

(including any viruses, worms, “logic bombs,” disabling codes, backdoors, subroutines, or expiration dates). The SUPPLIER shall provide SANOFI, upon request, with any evidence of the analysis performed;

- ПОСТАВЩИК должен строго контролировать доступ к исходному коду приложения;
- ПОСТАВЩИК обязан проводить проверку предоставленного приложения на наличие уязвимостей не реже одного раза в год и в любом случае до запуска приложения. ПОСТАВЩИК должен предоставить САНОФИ по его запросу любые доказательства проведения такой проверки;
- ПОСТАВЩИК должен обеспечить безопасность среды тестирования и разработки на том же уровне, что и безопасность рабочей среды;
- ПОСТАВЩИК должен обеспечить наличие в приложении возможности ограничения доступа к Данным Клиента (доступ только авторизованным пользователям);
- ПОСТАВЩИК должен обеспечить регистрацию приложением всех случаев получения доступа к Данным Клиента.

- The SUPPLIER shall strictly control access to application source code;
- The SUPPLIER is obliged to scan the provided application for vulnerabilities at least annually and in any case before the application is launched. The SUPPLIER shall provide SANOFI upon request with any evidence of such inspection;
- The SUPPLIER shall ensure the safety of the testing and development environment at the same level as the safety of the working environment;
- The SUPPLIER shall ensure the availability in the application of the possibility of restricting access to the Client's Data (access only to authorized users);
- The SUPPLIER shall ensure that the application registers all access to the Client Data.

4.2 Обслуживание и поддержка приложений

ПОСТАВЩИК обязан разрабатывать, обслуживать и поддерживать свое приложение и последующие обновления, новые версии и исправления ошибок таким образом, чтобы приложение было и оставалось защищенным от известных уязвимостей. Ни при каких обстоятельствах такие обновления, новые версии и исправления ошибок не могут снижать безопасность Услуг или Данных Клиента.

ПОСТАВЩИК обязуется предоставить САНОФИ уведомление не менее чем за 30 (тридцать) дней, если какое-либо обновление, новая версия или исправление ошибок в его приложениях или информационной среде может привести или приведет к последствиям для пользователя Услуг (скажется на работе пользователя, приведет к недоступности услуги и т. д.)

4.2 Maintenance and Support of Applications

The SUPPLIER shall develop, maintain, and support its application and subsequent updates, new versions, and bug fixes so that the application remains protected from known vulnerabilities. In no event may such updates, new versions or bug fixes compromise the security of the Services or Client Data.

The SUPPLIER shall provide SANOFI with at least thirty (30) days' notice if any update, new version, or bug fixes to its applications or information environment may result in, or result in, consequences for the user of the Services (affecting the user's performance, making the service unavailable, etc.)

4.3 Обеспечение отказоустойчивости приложений

ПОСТАВЩИК обязан обеспечить, чтобы предоставляемое им приложение было отказоустойчивым. К этим мерам могут относиться, помимо прочего, следующие:

- деактивация неиспользуемых или устаревших сервисов или функций программы;

4.3 Application fault tolerance assurance

The SUPPLIER shall ensure that the application provided by him is fault-tolerant. These measures may include, but are not limited to, the following:

- deactivation of unused or outdated services or functions of the application;

- изменение паролей администратора по умолчанию;
- по возможности, приложение не должно содержать в себе неконтролируемый исходный код, дополнения или плагины;
- строгий контроль за изменением конфигурации.

- changing the default administrator passwords
- if possible, the application should not contain uncontrolled source code, add-ons, or plug-ins.
- strict control over configuration changes.

4.4 Данные о разработке

В случае, когда ПОСТАВЩИК (или его Персонал) считается разработчиком / поставщиком / интегратором приложения:

- разработчик должен использовать или получать доступ к Данным Клиента исключительно по прямому запросу САНОФИ или с его одобрения, а также при наличии обоснованной установленной деловой потребности, подтвержденной САНОФИ; а также
- в среде разработки и испытаний должны использоваться псевдоанонимизированные или обезличенные данные.

4.4 Development data

Where the SUPPLIER (or its Personnel) is deemed to be the developer / supplier / integrator of the application:

- the Developer shall use or access the Client Data only upon SANOFI's express request or approval and when there is a reasonable established business need confirmed by SANOFI; and
- pseudo-anonymized or anonymized data shall be used in the development and test environment.

5. <u>Безопасность Данных Клиента</u>

5.1 Защита Данных Клиента

ПОСТАВЩИК обязан обеспечить шифрование всех Данных Клиента во время передачи вне зависимости от того, отправляются ли они через интернет или иным образом.

ПОСТАВЩИК обязан защищать все Данные Клиента, хранящиеся в базах данных, на серверах или других формах немобильных устройств, от всех разумно ожидаемых форм взлома с помощью шифрования, контроля логического доступа или других надежных мер обеспечения безопасности.

Персональные данные Клиента: по возможности, ПОСТАВЩИК должен либо зашифровать все Персональные данные, хранящиеся в неактивном состоянии, с отдельным управлением ключами, либо обезличить их, в результате чего повторная идентификация станет невозможна.

Если какие-либо Данные Клиента хранятся на каком-либо мобильном устройстве (включая, помимо прочего, портативные компьютеры, компакт-диски, планшетные компьютеры, внешние жесткие диски, резервные магнитные ленты и (или) съемные дискеты), такие данные должны быть в зашифрованном виде.

5. <u>Security of Client Data</u>

5.1 Protection of Client Data

The SUPPLIER shall ensure that all Client Data is encrypted during transmission, whether sent over the Internet or otherwise.

The SUPPLIER shall protect all Client Data stored in databases, servers or other forms of non-mobile devices from all reasonably expected forms of hacking by means of encryption, logical access control or other reliable security measures.

Client Personal Data: If possible, the SUPPLIER shall either encrypt all Personal Data stored in an inactive state, with separate key management, or anonymize them, making re-identification impossible.

If any Client Data is stored on any mobile device (including but not limited to laptops, CDs, tablets, external hard drives, backup tapes and/or removable floppies), such data shall be encrypted.

5.2 Резервное копирование Данных Клиента и конфигурации системы

В соответствии с Профессиональными стандартами ПОСТАВЩИК должен на регулярной основе выполнять резервное копирование Данных Клиента, соответствующего Журнала контроля и конфигурации системы. Резервные копии должны быть защищены от атак с криптоблокировкой.

ПОСТАВЩИК должен создавать как минимум две резервные копии в различных физически удаленных друг от друга местах.

Все резервные копии должны быть зашифрованы.

ПОСТАВЩИК должен провести проверку возможности восстановления данных за 3 (три) года и предоставить САНОФИ соответствующее документальное подтверждение.

- Если значительное ИТ-изменение в компьютеризированной системе влияет на функциональность / Услуги / параметры резервного копирования и возможности восстановления, ПОСТАВЩИК должен применить процесс управления ИТ-изменениями (как описано в разделе 1.9 «Управление ИТ-изменениями» настоящего документа) и провести новую проверку возможности восстановления.
- По запросу САНОФИ ПОСТАВЩИК должен предоставить документальное подтверждение начала и завершения задания по резервному копированию в соответствии с планом.

5.2 Backup of Client Data and System Configuration

In accordance with the Professional Standards, the SUPPLIER shall regularly back up the Client Data, the relevant Audit Trail and the system configuration. Backups must be protected against cryptoblocking attacks.

The SUPPLIER shall create at least two backups in different physically separated locations.

All backups must be encrypted.

The SUPPLIER shall check the recoverability of the data in three (3) years and provide SANOFI with the relevant documentary evidence.

- If a significant IT change to a computerized system affects the functionality / Services /Backup and Recovery Options, the SUPPLIER shall implement an IT Change Management process (as described in Section 1.9, IT Change Management, of this document) and conduct a new Recovery Verification.
- At the request of SANOFI, the SUPPLIER shall provide documentary evidence of the beginning and completion of the backup task in accordance with the plan.

5.3 Ограничение на использование Третьими лицами

Никакие Данные Клиента не могут быть проданы, переданы, сданы в аренду Третьим лицам или иным образом стать объектом распоряжения ПОСТАВЩИКОМ или использоваться в коммерческих целях ПОСТАВЩИКОМ или от его имени.

5.3 Restriction on use by Third Parties

No Client Data may be sold, transferred, leased to Third Parties or otherwise disposed of by or on behalf of the SUPPLIER or used for commercial purposes by or on behalf of the SUPPLIER.

6. <u>Безопасность Персонала</u>

6.1 Разделение обязанностей в области ИТ

ПОСТАВЩИК обязан реализовать разделение обязанностей в области информационных технологий. ПОСТАВЩИК обязан разделять задачи своего Персонала в соответствии с их должностными обязанностями.

6. <u>Personnel Safety</u>

6.1 Segregation of IT responsibilities

The SUPPLIER shall implement the division of responsibilities in the field of information technology. The SUPPLIER shall share the tasks of its Personnel in accordance with their duties.

6.2 Программа обучения и повышения осведомленности в области информационной безопасности

В течение срока действия Соглашения ПОСТАВЩИК обязуется проводить и поддерживать в актуальном состоянии программу обучения и информирования своего Персонала относительно их обязательств по обеспечению информационной безопасности.

Если ПОСТАВЩИК осуществляет сбор, предоставление, хранение, передачу или обработку каким-либо образом Данных Клиента, эта программа должна содержать раздел, посвященный защите Данных Клиента. ПОСТАВЩИК обязан обеспечить регулярное участие в такой программе всего своего Персонала, принимающего участие в проекте и (или) оказании Услуг.

6.2 Training and awareness raising program on information security

During the term of the Contract, the SUPPLIER undertakes to conduct and maintain an up-to-date program of training and informing its Personnel about their obligations to ensure information security.

If the SUPPLIER collects, provides, stores, transfers or processes in any way the Client Data, this program shall contain a section devoted to the protection of the Client Data. The SUPPLIER shall ensure that all of its Personnel involved in the project and/or the provision of Services participate in such a program on a regular basis.

6.3 Освобождение Персоналом ПОСТАВЩИКА своего рабочего места

При расторжении по какой-либо причине договора, связывающего Персонал и ПОСТАВЩИКА, ПОСТАВЩИК обязан грамотно организовать процесс освобождения сотрудником своего рабочего места с точки зрения информационной безопасности.

К этим мерам могут относиться, помимо прочего, следующие:

- правильная деактивация всех логических и физических учетных данных Персонала;
- возврат всего Оборудования и Данных Клиента;
- если Данные Клиента по какой-либо причине хранились локально на рабочей станции или мобильном устройстве Персонала, данные с жесткого диска и (или) запоминающих устройств должны быть гарантированно стерты.

6.3 SUPPLIER's Personnel vacating their workplace

In the event of termination for any reason of the contract linking the Personnel and the SUPPLIER, the SUPPLIER shall competently organize the process of the employee's vacation of his workplace from the point of view of information security.

These measures may include, but are not limited to, the following:

- correct deactivation of all logical and physical credentials of the Personnel;
- return of all Equipment and Client Data;
- if Client Data has for any reason been stored locally on a workstation or mobile device of the Personnel, the data from the hard disk and/or storage devices shall be guaranteed to be erased.

7. <u>Расторжение Соглашения</u>

7. <u>Termination of the Contract</u>

7.1 Возврат, уничтожение или санация Данных Клиента

Если иное не предусмотрено законом или нормативными актами, при расторжении Соглашения по любой причине ПОСТАВЩИК прекращает обработку любых Данных Клиента от имени САНОФИ и, по выбору САНОФИ, либо возвращает САНОФИ все Данные Клиента и любые их копии, которые он обрабатывает, обработал или обрабатывал от имени САНОФИ в формате, согласованном с САНОФИ, либо уничтожает Данные Клиента по требованию САНОФИ или санирует данные в среде ПОСТАВЩИКА и предоставляет доказательства

7.1 Return, Destruction or Sanitation of Client Data

Unless otherwise required by law or regulation, upon termination of the Contract for any reason, SUPPLIER shall cease processing any Client Data on behalf of SANOFI and, at SANOFI's discretion, either return to SANOFI all Client Data and any copies thereof that it processes, has processed or has processed on behalf of SANOFI in a format agreed with SANOFI, or destroy Client Data as requested by SANOFI or sanitize the data within the SUPPLIER's environment and provide evidence of such sanitization or destruction of Client Data within fifteen (15) days after completion of the Services (except

такой санации или уничтожения Данных Клиента в течение 15 (пятнадцати) дней по окончании оказания Услуг (если иное не предусмотрено Соглашением).

as otherwise provided in the Contract).

7.2 Возврат оборудования

7.2 Return of equipment

При расторжении Соглашения по любой причине все оборудование САНОФИ подлежит возврату в течение 30 (тридцати) дней с момента расторжения Соглашения.

Upon termination of the Contract for any reason, all SANOFI equipment shall be returned within thirty (30) days from the termination of the Contract.

8. <u>Аудит и контроль информационной безопасности и качества</u>

8. <u>Information security and quality audit and monitoring</u>

8.1 Право на проведение аудита

8.1 Right to Audit

САНОФИ или назначенная им аудиторская фирма имеет право проводить аудит ПОСТАВЩИКА и осуществлять любые меры контроля, которые будут сочтены подходящими для обеспечения соблюдения обязательств ПОСТАВЩИКА по обеспечению информационной безопасности и качества. Для этой цели ПОСТАВЩИК должен предоставить представителям САНОФИ доступ для целей аудита в соответствующие помещения и объекты и соглашается предоставлять документацию и доказательства.

SANOFI or its appointed audit firm shall have the right to audit the SUPPLIER and to implement any controls deemed appropriate to ensure that the SUPPLIER's information security and quality obligations are met. For this purpose, the SUPPLIER shall provide SANOFI's representatives with access for the purposes of the audit to the relevant premises and facilities and agrees to provide documentation and evidence.

Кроме того, САНОФИ имеет право проводить аудит субподрядчиков ПОСТАВЩИКА и их систем; это не освобождает ПОСТАВЩИКА от принятия всех обоснованных мер для проверки соблюдения его субподрядчиками положений настоящего документа.

In addition, SANOFI has the right to audit the SUPPLIER's subcontractors and their systems; this does not release the SUPPLIER from taking all reasonable steps to verify its subcontractors' compliance with the provisions of this document.

САНОФИ обеспечит минимальное вмешательство в деятельность ПОСТАВЩИКА.

SANOFI will ensure minimal interference in the SUPPLIER's activities.

Этот вид контроля осуществляется согласно соответствующим положениям Соглашения (при наличии таковых).

This control shall be carried out in accordance with the relevant provisions of the Agreement (if any).

8.2 Информационная безопасность

8.2 Information Security

8.2.1 Ежегодная оценка системы информационной безопасности

8.2.1 Annual assessment of the information security system

В дополнение к вышеизложенному ПОСТАВЩИК обязан каждый календарный год привлекать за собственный счет известную в стране аудиторскую фирму, указанную САНОФИ или предложенную ПОСТАВЩИКОМ, для проведения аудита, который должен охватывать как минимум политики и процедуры ПОСТАВЩИКА в области обеспечения безопасности, а также средства контроля, включая безопасность облачных сервисов и данных. По запросу САНОФИ ПОСТАВЩИК обязан предоставить САНОФИ копию такого отчета.

In addition to the above, the SUPPLIER shall engage at its own expense each calendar year a nationally known audit firm designated by SANOFI or proposed by the SUPPLIER to conduct an audit which shall cover at a minimum the SUPPLIER's security policies and procedures and controls, including the security of cloud services and data. Upon SANOFI's request, the SUPPLIER shall provide SANOFI with a copy of such report.

8.2.2 План устранения недостатков

Если в ходе аудита будут выявлены какие-либо нарушения или недостатки в соответствии с настоящим Соглашением или если после аудита САНОФИ будут даны рекомендации или возражения, ПОСТАВЩИК обязуется незамедлительно и за свой счет (i) реализовать план устранения этих нарушений и (или) недостатков; (ii) выполнить рекомендации и ответить на возражения САНОФИ.

8.2.2 Defects Liability Plan

If the audit reveals any irregularities or deficiencies under this Contract or if recommendations or objections are made after the audit of SANOFI, the SUPPLIER shall promptly (i) implement, at its own expense, a plan to remedy those irregularities and/or deficiencies; (ii) implement the recommendations and respond to SANOFI's objections.

8.3 Аудит качества

В рамках процесса предварительного отбора и на регулярной основе, но не чаще одного раза в год, САНОФИ может использовать право на проведение аудита (выездного или по почте с использованием анкеты).

Кроме того, при обнаружении существенных проблем в отношении Услуг, предоставляемых ПОСТАВЩИКОМ, ПОСТАВЩИК уполномочивает САНОФИ на проведение необходимой проверки причины, что позволит найти решение этих проблем.

После предоставления САНОФИ аудиторского отчета ПОСТАВЩИК должен предоставить план устранения недостатков и (или) корректирующих и предупреждающих действий в отношении критических результатов в течение 15 (пятнадцати) рабочих дней с момента получения любого официального запроса (аудиторского отчета, контрольной документации и т. д.). В отношении аудиторских отчетов, не содержащих критических результатов, ПОСТАВЩИК должен предоставить ответ в течение 20 (двадцати) рабочих дней.

Для систем, регулируемых Законом Сарбейнза–Оксли, в дополнение к вышеизложенному ПОСТАВЩИК обязан каждый календарный год привлекать за собственный счет известную в стране аудиторскую фирму, соответствующую требованиям САНОФИ, для проведения аудита, который должен охватывать как минимум политики и процедуры ПОСТАВЩИКА в области обеспечения качества, а также соответствующие средства контроля. По запросу САНОФИ ПОСТАВЩИК должен предоставить САНОФИ копию такого отчета, например формат SSAE-16 SOC 2 Type II.

8.3 QA/QC audit

As part of the pre-selection process and on a regular basis, but not more than once a year, SANOFI can exercise the right to audit (on-site or by mail using a questionnaire).

In addition, if material problems are identified in relation to the Services provided by the SUPPLIER, the SUPPLIER authorizes SANOFI to carry out the necessary root cause verification to find a solution to these problems.

Upon submission of the audit report to SANOFI, the SUPPLIER shall submit a remedial and/or corrective and preventive action plan for critical results within fifteen (15) business days from receipt of any formal request (audit report, control documentation, etc.). For audit reports that do not contain critical results, the SUPPLIER shall provide a response within twenty (20) business days.

For systems governed by the Sarbanes-Oxley Act, in addition to the foregoing, the SUPPLIER shall engage, at its own expense, a SANOFI-compliant audit firm known in the country, each calendar year to conduct an audit that shall cover, as a minimum, the SUPPLIER's quality assurance policies and procedures and the appropriate controls. Upon request by SANOFI, the SUPPLIER shall provide SANOFI with a copy of such report, such as SSAE-16 SOC 2 Type II format.

8.4 Надзор со стороны ПОСТАВЩИКА над субподрядчиками

ПОСТАВЩИК обязуется обеспечить постоянный контроль за задачами, выполнение которых было поручено его уполномоченным субподрядчикам.

8.4 The SUPPLIER Supervision of Subcontractors

The SUPPLIER undertakes to ensure constant monitoring of the tasks entrusted to its authorized subcontractors.

9. Аварийное восстановление и обеспечение непрерывности деятельности

ПОСТАВЩИК должен своевременно уведомлять САНОФИ о том, что Сервисы будут недоступны для проведения планового обслуживания или модернизации.

ПОСТАВЩИК несет ответственность за разработку и тестирование стратегии на случай непредвиденных обстоятельств / обеспечения непрерывности деятельности / аварийного восстановления, позволяющей обеспечить предоставление Услуг САНОФИ, если ПОСТАВЩИК окажется в чрезвычайных обстоятельствах или пострадает от них. ПОСТАВЩИК должен предоставить САНОФИ по его запросу соответствующий отчет о проведенном тестировании.

ПОСТАВЩИК должен сохранить возможность продолжать предоставлять Услуги в случае чрезвычайных обстоятельств и задействовать альтернативные механизмы обеспечения доступа САНОФИ к Услугам.

В случае внеплановой недоступности Услуг ПОСТАВЩИК должен проинформировать САНОФИ и совместными с ним усилиями оценить воздействие недоступных Услуг (включая причины, влияние на Услуги и предполагаемую продолжительность этого события).

9. Disaster recovery and business continuity

The SUPPLIER shall promptly notify SANOFI that the Services will not be available for scheduled maintenance or upgrades.

The SUPPLIER shall be responsible for developing and testing a Contingency / Business Continuity / Disaster Recovery strategy to enable the provision of SANOFI Services in the event that the SUPPLIER is in, or suffers from, an emergency. The SUPPLIER shall provide SANOFI with an appropriate test report upon request.

The SUPPLIER shall retain the ability to continue to provide the Services in the event of an emergency and shall use alternative mechanisms to ensure SANOFI's access to the Services.

In the event of unplanned unavailability of the Services, the SUPPLIER shall inform SANOFI and jointly assess the impact of unavailable Services (including the reasons, impact on the Services and the estimated duration of this event).

10. Обязанности и обязательства в области качества (применимы к компьютеризированным системам GxP и (или) компьютеризированным системам, регулируемым Законом Сарбейнза–Оксли)

10.1 Роли и обязанности

ПОСТАВЩИК должен предоставить САНОФИ и поддерживать в актуальном состоянии оформленный в письменной форме список лиц из числа Персонала, задействованного в интерфейсах связи в целях обеспечения качества.

10.2 Обязательства

ПОСТАВЩИК обязан предоставлять САНОФИ Услуги в соответствии с (i) требованиями GxP, (ii) приложением 11 том 4 Европейской надлежащей производственной практики в отношении компьютеризированных систем GxP, (ii) главой 21 Свода федеральных правил Часть 11 Управления по контролю качества пищевых продуктов и лекарственных средств США в отношении

10. Quality Assurance Responsibilities and Obligations (Applicable to GxP Computerized Systems and/or Sarbanes-Oxley Computerized Systems)

10.1 Roles and Responsibilities

The SUPPLIER shall provide to SANOFI and keep up to date a written list of persons from among the Personnel involved in the communication interfaces for the purpose of quality assurance.

10.2 Liabilities

The SUPPLIER shall provide SANOFI with the Services in accordance with (i) GxP Requirements, (ii) Appendix 11 of Volume 4 of the European Good Manufacturing Practice for GxP Computerized Systems, (ii) Chapter 21 of the US FDA Part 11 Code of Federal Regulations for Electronic Records and Electronic Signatures.

электронных записей и электронных подписей.

ПОСТАВЩИК обязуется принять все разумные меры для обеспечения разработки и подтверждения пригодности Услуг, предоставляемых САНОФИ, для использования по назначению и в соответствии с надлежащей системой управления качеством.

The SUPPLIER undertakes to take all reasonable measures to ensure the development and confirmation of the suitability of the Services provided by SANOFI for its intended use and in accordance with a proper quality management system.

ПОСТАВЩИК должен предоставить по запросу САНОФИ объективные доказательства соблюдения требований настоящего документа.

The SUPPLIER must provide, at SANOFI's request, objective evidence of compliance with the requirements of this document.

ПОСТАВЩИК обязуется обеспечить наличие у всего Персонала, участвующего в предоставлении компьютеризированных систем и (или) оказании Услуг в соответствии с Соглашением, квалификации, необходимой для выполнения своих должностных обязанностей.

The SUPPLIER undertakes to ensure that all Personnel involved in the provision of computerized systems and/or the provision of Services in accordance with the Contract have the qualifications necessary for the performance of their official duties.

ПОСТАВЩИК должен предоставить доказательства полученного образования и прохождения обучения по любым соответствующим нормативным положениям, стандартам и процессам, применимым к Персоналу, участвующему в оказании Услуг.

The SUPPLIER shall provide evidence of education and training of Personnel involved in the provision of the Services in any relevant regulations, standards, and processes applicable.

ПОСТАВЩИК должен обеспечить адекватное ведение журналов контроля для всех применимых записей GxP (то есть записей по доступу пользователей, основных данных, динамических данных и т. д.) в соответствии с соглашением с САНОФИ.

The SUPPLIER shall ensure that audit trails are adequately maintained for all applicable GxP records (i.e., user access records, master data, dynamic data, etc.) as per SANOFI agreement.

ПОСТАВЩИК должен разработать, контролировать, а также, при необходимости, дорабатывать и актуализировать содержание комплексного Плана обеспечения качества (в письменном виде). План обеспечения качества должен описывать способ реализации ПОСТАВЩИКОМ , если это применимо, каждой меры обеспечения качества, перечисленной в настоящем документе. План обеспечения качества должен быть утвержден САНОФИ до начала оказания Услуг.

The SUPPLIER shall develop, control, and, if necessary, finalize and update the content of the comprehensive Quality Assurance Plan (in writing). The quality assurance plan shall describe how the SUPPLIER will implement, if applicable, each quality assurance measure listed in this document. The Quality Assurance Plan must be approved by SANOFI prior to the commencement of the Services.

10.3 Инцидент, влияющий на целостность или соответствие требованиям Данных Клиента (не относится к инцидентам, связанным с безопасностью и персональными данными)

10.3 Incident affecting the integrity or compliance with the requirements of the Client Data (not applicable to security and personal data incidents)

ПОСТАВЩИК обязуется выявлять и регистрировать любой Инцидент, влияющий на целостность Данных Клиента или влияющий на соответствие требованиям, функциональность или доступность предоставляемых Услуг. ПОСТАВЩИК должен применять процесс работы с Инцидентами.

The SUPPLIER shall identify and record any Incident that affects the integrity of the Client Data or affects the compliance, functionality or availability of the Services provided. The SUPPLIER shall apply the Incident Management Process.

ПОСТАВЩИК обязан обеспечить эффективную и оперативную обработку Инцидента, влияющего на целостность Данных Клиента или влияющего на

The SUPPLIER shall ensure that an Incident affecting the integrity of Client Data or affecting the compliance, functionality or availability of the Services is handled

соответствие требованиям, функциональность или доступность Услуг, и в разумные сроки сообщить САНОФИ об обнаружении критического Инцидента.

ПОСТАВЩИК должен реализовать план устранения нарушений и (или) план корректирующих и предупреждающих действий для устранения Инцидента и предотвращения аналогичного события в будущем.

efficiently and expeditiously and shall notify SANOFI within a reasonable time of the discovery of a critical Incident.

The SUPPLIER shall implement a corrective action plan and/or a corrective and preventive action plan to correct the Incident and prevent a similar event in the future.

10.4 Проверки и запросы регуляторных органов, а также внутренний аудит САНОФИ

Если какая-либо Сторона получит уведомление о какой-либо проверке или запросе со стороны регуляторного органа или проведении внутреннего аудита САНОФИ по вопросам, имеющим непосредственное отношение к Услугам, предоставляемым ПОСТАВЩИКОМ, такая Сторона должна незамедлительно проинформировать другую Сторону о любой такой проверке, аудите или запросе регуляторного органа.

В этом случае ПОСТАВЩИК должен разрешить уполномоченному лицу САНОФИ присутствовать по требованию ПОСТАВЩИКА.

ПОСТАВЩИК соглашается с тем, что во время любой такой проверки регуляторного органа он должен санкционировать любую проверку своих процессов, документов и помещений регуляторными органами или от их имени и должен предоставить доступ к ресурсам, которые позволят получить ответы на запросы любых инспекторов. Хранящиеся у ПОСТАВЩИКА документы должны быть готовы к проверке.

ПОСТАВЩИК соглашается с тем, что во время внутреннего аудита САНОФИ ПОСТАВЩИК должен предоставить доступ к ресурсам, которые позволят получить ответы на запросы внутренних аудиторов САНОФИ.

ПОСТАВЩИК не должен взимать с САНОФИ плату за время, затраченное на содействие инспекторам (или) аудиторам во время таких проверок.

10.4 Regulatory audits and inquiries and SANOFI's internal audit

Should either Party be notified of any inspection or request by a regulatory authority or the conduct of an internal audit by SANOFI on matters directly related to the Services provided by the SUPPLIER, such Party shall promptly inform the other Party of any such inspection, audit or request by the regulatory authority.

In this case, the SUPPLIER shall allow the authorized person of SANOFI to be present at the request of the SUPPLIER.

The SUPPLIER agrees that at the time of any such inspection of a regulatory authority, it shall authorize any inspection of its processes, documents, and premises by or on behalf of regulatory authorities and shall provide access to resources that will permit responses to requests of any inspectors. The documents kept by the SUPPLIER shall be ready for inspection.

The SUPPLIER agrees that during the internal audit of SANOFI, the SUPPLIER shall provide access to resources that will allow responses to requests of SANOFI's internal auditors.

The SUPPLIER shall not charge SANOFI for the time spent assisting inspectors (or auditors) during such inspections.