

**Master Service Agreement for the Use
of teamplay
(The Republic of Kazakhstan, Version: June 1st, 2020)**

0. Definitions

In this document the following terms shall have the meaning set out below:

"Account" shall mean the account of the Institution ("Institution Account") or the Individual User ("User Account") entitling the Institution and the Individual User to access the Services.

"Data" shall mean Personal Data and Network Data.

"Database" shall mean the cloud-based Azure platform operated by Microsoft.

"Data Processing Annex" shall mean the Annex on the Processing of Personal Data entered into between the Institution and Siemens Healthcare.

"Individual User" shall mean the individual physician or medical physicists as well as other personnel of the Institution that needs access to the Services for the performance of their job obligations.

"Institution" shall mean the institution, hospital or other legal entity having been registered online by an Individual User.

"MSA" shall mean this Master Service Agreement for the use of teamplay having been accepted online by an Individual User on behalf of the Institution.

"Network Data" shall mean any data being extracted from the connected devices or sent by Individual Users and shall include any (analytical) result of the Services. Network Data shall be excluding Personal Data but including anonymized Personal Data.

"Personal Data" shall mean any information relating to an identified or identifiable natural person, including such personal data related to patients and employees of the Institution.

"Privacy Notice" shall mean the privacy notice being accepted online by Individual Users.

"Processing" or "Process" means any operation or set of operations which is performed on Data or on sets of Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Receiver" shall mean the receiver software being downloaded by the Institution to its IT infrastructure.

"Receiver Terms" shall mean the license schedule attached to the MSA.

"Services" shall mean the services available at <https://teamplay.siemens.com> and all sub domains and any subsequent domains.

"Siemens" shall mean Siemens Healthcare LLP, 22/5 Khadzhy Mukan str., 050059, Almaty, Kazakhstan, 'service.kz@siemens-healthineers.co.

"Siemens Healthcare" shall mean Siemens Healthcare GmbH, Henkestr. 127, 91052 Erlangen, Germany.

**Генеральное соглашение о предоставлении услуг по
использованию платформы teamplay
(Республика Казахстан, Версия: 01 июня 2020 г.)**

0. Определения

Указанные термины в данном документе будут иметь следующие значения.

«Учетная запись» означает учетную запись Учреждения (далее «Учетная запись учреждения») или Отдельного пользователя (далее «Учетная запись пользователя»), которая дает право Учреждению и Отдельному пользователю получать доступ к Услугам.

«Данные» означают Персональные данные и Сетевые данные.

«База данных» означает облачную платформу Azure компании Microsoft.

«Приложение об обработке данных» означает Приложение об обработке Персональных данных, которое заключается между Учреждением и компанией «Сименс Здравоохранение».

«Отдельный пользователь» означает отдельного врача или медицинских физиков, а также других сотрудников Учреждения, которым необходим доступ к Услугам для выполнения своих служебных обязанностей.

«Учреждение» означает учреждение, больницу или другое юридическое лицо, которое было зарегистрировано в режиме онлайн Отдельным пользователем.

«ГСПУ» означает настоящее Генеральное соглашение о предоставлении услуг по использованию платформы teamplay, условия которого были приняты в режиме онлайн Отдельным пользователем от имени Учреждения.

«Сетевые данные» означают любые данные, извлеченные из подключенных устройств или отправленные Отдельным пользователем, а также любой (аналитический) результат Услуг. Сетевые данные не включают в себя Персональные данные, за исключением обезличенных Персональных данных.

«Персональные данные» означают любую информацию об определенном или определяемом физическом лице, включая персональные данные, имеющие отношение к пациентам и сотрудникам Учреждения.

«Уведомление о конфиденциальности» означает уведомление о конфиденциальности, условия которого были приняты в режиме онлайн Отдельными пользователями.

«Обработка» или «Обрабатывать» означает любую операцию или ряд операций, которые производятся с Данными или с набором Данных, с использованием автоматизированных средств или без них, включая сбор, запись, организацию, структуризацию, хранение, уточнение или изменение, извлечение, консультацию, использование, раскрытие путем передачи, распространение или предоставление иным образом, совмещение или комбинацию, ограничение, стирание или уничтожение.

«Получатель» означает программу-получатель, загруженную Учреждением в свою ИТ-инфраструктуру.

«Условия получателя» означают лицензионное дополнение, прилагаемое к настоящему ГСПУ.

«Услуги» означают услуги, доступные на сайте <https://teamplay.siemens.com>, во всех субдоменах и любых последующих доменах.

«Сименс» означает ТОО «Сименс Здравоохранение», Республика Казахстан, 050059, г. Алматы, ул. Хаджи Мукана 22/5, service.kz@siemens-healthineers.co «Сименс Здравоохранение» (Siemens Healthcare) означает компанию «Сименс Хелскэа ГмбХ» (Siemens

“Subscription” shall mean free-of-charge subscriptions (“Basic Subscription”), premium trial subscriptions (“Trial Subscription”) or paid subscriptions (“Paid Subscription”).

“teampay” shall mean the web-based platform offering the Services.

“Third Party Provider” shall mean a provider other than Siemens or Siemens Healthcare of Third-Party Solutions.

“Third Party Solution” shall mean a solution such as an application, service or software offered and provided by a Third Party Provider.

1. Scope of the MSA

This MSA shall govern the contractual relationship between the Institution and Siemens. This MSA shall govern any Subscription.

This MSA, except the Data Processing Annex, does not govern the contractual relationship between the Institution and Siemens Healthcare. The contractual relationship between the Institution and Siemens Healthcare is exclusively governed by the Data Processing Annex.

Siemens shall under no circumstances Process any kind of Personal Data in connection with the provision of the Services. Any Processing of Personal Data shall be undertaken only by Siemens Healthcare (and/or its sub-contractors) in accordance with the provisions of the Data Processing Annex entered into between the Institution and Siemens Healthcare.

2. Subject Matter

2.1 teampay provides a web based platform for medical professionals that will (some features might not be available from start) (i) provide the Institution / the Individual Users with Services based on data analytics, (ii) support Individual Users to build a global clinical network, (iii) provide an online community to work in virtual groups and (iv) provide Individual Users with tools for secure online data and image (DICOM) review, transfer and sharing (v) enable access to Third Party Solutions offered by Third Party Providers subject to separate agreements (collectively “Intended Use”).

The Institution and the Individual Users will be provided with Services based on data analytics through the processing of the Data by Siemens Healthcare on behalf of the Institution. Such Services include (a) the creation of statistical analyses (e.g. average doses, image analytics) in order to improve imaging methods in connection with the treatment of patients and for quality assurance and quality management, particularly to reduce the radiation exposure in connection with imaging methods; as well as to improve utilization, examination processes and capacity planning and (b) the calculation and creation of benchmark values (e.g. average dose consumptions) for other institutions and (c) the development and improvement of utilities and applications to improve systems of the hospital and the treatment of patients. For Siemens Healthcare’s Processing of

Healthcare GmbH), Henkestr. 127, 91052 Erlangen, Germany (Германия).

«Подписка» означает бесплатные подписки (далее — «Базовая подписка»), пробные премиум-подписки (далее — «Пробная подписка») или платные подписки (далее — «Платная подписка»).

«teampay» означает веб-платформу, где предлагаются Услуги.

«Сторонний провайдер» означает любого провайдера сторонних решений, кроме компании «Сименс» или компании «Сименс Здравоохранение».

«Стороннее решение» означает решение, включая приложение, услугу или программное обеспечение, предложенное Сторонним провайдером.

1. Область действия ГСПУ

Настоящее ГСПУ регулирует контрактные отношения между Учреждением и компанией «Сименс». Настоящее ГСПУ регулирует любые Подписки.

Настоящее ГСПУ, кроме Приложения об обработке данных, не регулирует контрактные отношения между Учреждением и компанией «Сименс Здравоохранение». Контрактные отношения между Учреждением и компанией «Сименс Здравоохранение» регулируются исключительно Приложением об обработке данных.

Компания «Сименс» ни при каких обстоятельствах не будет обрабатывать Персональные данные, связанные с предоставлением Услуг. Любая Обработка Персональных данных будет проводиться только компанией «Сименс Здравоохранение» (и/или ее субподрядчиками) в соответствии с положениями Приложения об обработке данных, которое заключается между Учреждением и компанией «Сименс Здравоохранение».

2. Предмет соглашения

2.1. Веб-платформа teampay для медицинских работников (некоторые функции могут быть не доступны в начале) (i) предоставляет Учреждению/Отдельным пользователям Услуги, основанные на анализе данных, (ii) оказывает поддержку Отдельным пользователям при построении глобальной сети клиник, (iii) предоставляет онлайн-сообщество для работы в виртуальных группах, (iv) предоставляет Отдельным пользователям инструменты для безопасного просмотра, передачи и совместного использования данных и изображений (DICOM) в режиме онлайн, (v) предоставляет доступ к Сторонним решениям, которые предлагаются Сторонними провайдерами, при условии заключения отдельных соглашений (далее совместно — «Предусмотренное применение»).

Учреждению и Отдельным пользователям будут предоставлены Услуги на основании аналитических данных посредством обработки Данных компанией «Сименс Здравоохранение» от имени Учреждения. Такие Услуги включают (а) разработку статистических анализов (например, средняя дозировка, анализ изображений) для усовершенствования методов визуализации при лечении пациентов и для обеспечения качества и управления качеством, в особенности для снижения уровня воздействия радиации в рамках методов визуализации, а также для усовершенствования процедур использования, изучения и планирования загрузки; (б) расчет и создание базисных значений (например, средняя доза потребления) для других учреждений и (в) разработку и улучшение работы коммунального сектора

Data for purposes beyond the aforementioned Intended Use, Personal Data will be anonymized. The anonymization of Personal Data will be Processed in the Database.

2.2 Certain applications or application features (e.g. teamplay Images) may be classified as a medical device in certain jurisdictions. Otherwise teamplay is not a medical product. TEAMPLAY IS NOT INTENDED FOR PRIMARY DIAGNOSIS, AND IS NOT INTENDED FOR DETAILED TREATMENT PLANNING OR TREATMENT OF PATIENTS. The Services are not intended to replace clinical decisions, provide medical advice or endorse any particular radiation plan or treatment regimen. The patient's medical professionals are solely responsible for and must rely on their professional clinical judgment when deciding how to plan and provide treatment. teamplay or the Services are not a substitute for Institution's primary data sources and are not for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease. Siemens or Siemens Healthcare are not authorized or qualified to engage in activities that may be construed or deemed to constitute the practice of medicine.

2.3 teamplay is provided exclusively for use by Individual Users upon online registration and acceptance of the Privacy Notice, for use in their course of professional activities only.

2.4 Upon installation, the Receiver will Process the extraction of Data from the connected devices or will be ready to Process Data being pushed by Individual Users and perform Data minimization, according to the settings of the Receiver and upload Data to the Database.

3. Registration

3.1 The Institution shall control access of Individual Users to teamplay. The Institution agrees that teamplay is proprietary to Siemens and the Institution shall not grant access to teamplay to competitors of Siemens.

3.2 The Institution further agrees and ensures that each Individual User shall:

- a. Register prior to using teamplay by entering all user information requested as part of the registration process and by accepting the Privacy Notice;
- b. Not use pseudonyms or pen names;
- c. Provide only accurate and complete information for registration purposes ("Registration Data");
- d. Correct the Registration Data without undue delay in the event of any changes in the Registration Data;
- e. Provide adequate proof to verify his or her Registration Data if so requested by Siemens, with the acknowledgment that Siemens may disable access to an Individual User account until receipt of such proof;

и приложений для усовершенствования систем больницы и лечения пациентов. Персональные данные будут обезличены в случае Обработки данных компанией «Сименс Здравоохранение» для целей, которые выходят за рамки Предусмотренного применения. Персональные данные будут обезличиваться при Обработке в Базе данных.

2.2. Определенные приложения или их характеристики (например, teamplay Images) могут быть классифицированы в качестве медицинского изделия в некоторых юрисдикциях. В иных случаях платформа teamplay не является медицинским продуктом. ПЛАТФОРМА TEAMPLAY НЕ ПРЕДНАЗНАЧЕНА ДЛЯ ПОСТАНОВКИ ПЕРВИЧНОГО ДИАГНОЗА И ТАКЖЕ НЕ ПРЕДНАЗНАЧЕНА ДЛЯ ДЕТАЛЬНОГО ПЛАНИРОВАНИЯ ЛЕЧЕНИЯ ИЛИ ЛЕЧЕНИЯ ПАЦИЕНТОВ. Услуги не предназначены для замены клинических решений, предоставления медицинских рекомендаций или утверждения программы радиотерапии или схемы лечения. Медицинские сотрудники несут единоличную ответственность и обязаны полагаться на свою профессиональную клиническую оценку при принятии решения о планировании и предоставлении лечения. Платформа teamplay или Услуги не являются заменой основным источникам данных Учреждения и не предназначены для диагностики болезней или других состояний, а также для излечения, ослабления, лечения или предотвращения болезни. Компании «Сименс» и «Сименс Здравоохранение» не имеют права принимать участие в тех видах деятельности, которые могут быть истолкованы или восприняты, как медицинская деятельность.

2.3. Платформа teamplay предоставляется исключительно для использования Отдельными пользователями после онлайн-регистрации и принятия Уведомления о конфиденциальности только для применения в своей профессиональной практике.

2.4. После установки Получатель извлечет Данные из подключенных устройств или будет готов к Обработке данных, предоставленных Отдельными пользователями, осуществит минимизацию Данных в соответствии с настройками Получателя и загрузит Данные в Базу данных.

3. Регистрация

3.1. Учреждение обязуется контролировать доступ Отдельных пользователей к платформе teamplay. Учреждение согласно с тем, что права на платформу teamplay принадлежат компании «Сименс», и Учреждение обязуется не предоставлять доступ к платформе teamplay конкурентам компании «Сименс».

3.2. Учреждение также гарантирует, что каждый Отдельный пользователь обязуется:

- а) зарегистрироваться перед использованием платформы teamplay путем внесения всех данных о пользователе, которые требуются в рамках регистрационного процесса, и путем принятия Уведомления о конфиденциальности;
- б) не использовать псевдонимы или прозвища;
- в) предоставлять только точные и полные данные для регистрации (далее «Регистрационные данные»);
- г) своевременно корректировать Регистрационные данные в случае их изменения;
- д) предоставлять необходимые подтверждающие сведения для проведения проверки Регистрационных данных, если таковые будут запрошены компанией «Сименс», с учетом того, что компания «Сименс» имеет право отказать в доступе любому Отдельному пользователю до получения таких подтверждающих сведений;

f. Keep his or her password secret at all times, and avoid disclosing such password to any third party or to Siemens (Siemens will not ask for any passwords at any time);

g. Only establish one (1) user Account and may not share such account with any other user or any other individual; and

h. Be responsible for the contents of all information posted, submitted or otherwise disclosed by such Individual User.

4. Restrictions on Use

4.1 teamplay shall not be used for any purpose that is unlawful or prohibited by this MSA. The Institution shall comply, and shall ensure that its Individual Users comply, with all applicable laws, treaties, regulations and third-party rights, including, without limitation, those local, state, national and foreign laws related to data privacy, international communications, the transmission of technical or personal information, and government regulations. The Institution is solely responsible for the use or the misuse of teamplay by Individual Users.

4.2 The Institution shall be responsible for obtaining and maintaining technical equipment, resources and other requirements needed to access and use teamplay, including but not limited to computer hardware, software, communication devices and internet access ("Equipment"). For the avoidance of doubt, Equipment does not include the Receiver. Any costs arising out of or in connection with the Equipment shall be borne by the Institution.

4.3 Without limiting the foregoing, Siemens may disable, restrict access to or the availability of teamplay if it determines any of the restrictions on use have been violated. Siemens may also delete any content, information or other material that Siemens deems to be illegal, offensive or otherwise in violation with this MSA.

4.4 If the Institution installs Receivers at affiliated institutions outside of the country where the Institution is located, the Institution holds Siemens and Siemens Healthcare harmless from any damages resulting from breaches of the law applicable to such affiliated institution. Siemens is prepared to request from Siemens Healthcare to enter into a data processing agreement with such affiliated institution.

4.5 The Institution shall limit access to Services being classified as a medical device (e.g. teamplay Images) to Individual Users having been trained with respect to the use of such Service. The Institution shall ensure that Individual Users understand the instruction for use being accessible in teamplay.

е) всегда сохранять в тайне свой пароль и избегать раскрытия такого пароля любым третьим лицам или компании «Сименс» (компания «Сименс» никогда не будет запрашивать ваши пароли);

ж) создавать только 1 (одну) пользовательскую Учетную запись и не использовать ее совместно с какими-либо другими пользователями или лицами и

з) нести ответственность за содержание всей информации, которую такой Отдельный пользователь публикует, предоставляет или раскрывает иным образом.

4. Ограничение использования

4.1. Платформа teamplay не будет использоваться для целей, которые являются незаконными или запрещены настоящим ГСПУ. Учреждение обязуется соблюдать и гарантирует, что ее Отдельные пользователи также будут соблюдать все действующие законы, договоры, положения и права третьих лиц, включая, среди прочего, местные, государственные, национальные и иностранные законы, связанные с конфиденциальными данными, международными связями, передачей технических и персональных данных, а также правительственные постановления. Учреждение единолично несет ответственность за использование или ненадлежащее использование Отдельными пользователями платформы teamplay.

4.2. Учреждение несет ответственность за получение и обслуживание технического оборудования, ресурсов и выполнение других требований, необходимых для получения доступа и использования платформы teamplay, включая без ограничения компьютерное оборудование, программное обеспечение, коммуникационные устройства и доступ в Интернет (далее — «Оборудование»). Во избежание сомнений Оборудование не включает в себя Получателя. Любые расходы, возникающие в связи с Оборудованием, компенсируются Учреждением.

4.3. Без ущерба для вышеизложенного компания «Сименс» может отключить или ограничить доступ к платформе teamplay, если будет установлен факт нарушения ее использования. Компания «Сименс» может также удалять любой контент, информацию или другие материалы, которые она посчитает незаконными, оскорбительными или иным образом нарушающими положения настоящего ГСПУ.

4.4. Если Учреждение устанавливает Получатели в аффилированных учреждениях за пределами страны, где находится само Учреждение, то оно гарантирует компаниям «Сименс» и «Сименс Здоровоохранение» компенсацию любого ущерба, нанесенного в результате нарушения законодательства, применимого к таким аффилированным учреждением. Компания «Сименс» готова требовать от компании «Сименс Здоровоохранение» заключить соглашение об обработке данных с таким аффилированным учреждением.

4.5. Учреждение обязуется предоставлять доступ к Услугам, которые классифицируются как медицинские изделия (например, teamplay Images), только тем Отдельным пользователям, которые были проинструктированы относительно использования такой Услуги. Учреждение проследит за тем, чтобы Отдельные пользователи понимают инструкции по использованию, которые доступны на платформе teamplay.

5. Subscriptions

5.1 Siemens offers various types of Subscriptions. Basic and Trial Subscriptions are provided at no cost and may be upgraded by the Institution to a Paid Subscription with premium subscription packages and/or subscription-based features subject to additional fees. Please contact a Siemens sales representative with regard to Paid Subscriptions.

5.2 Siemens will provide an offer for installation and/or configuration services upon request at Institution's cost. Siemens' support regarding the Receiver, teamplay and the Database are dependent on the type of Subscription.

6. Responsibility for Personal Data

6.1 Some of the Data provided by the Institution may qualify as Personal Data as regulated by the Law of the Republic of Kazakhstan on Personal Data and its Protection dated 21 May 2013. In this regard, the Institution shall comply with its obligations as Controller under any and all applicable local and/or European Union data protection laws and regulations as well as with all applicable professional and criminal law requirements for the protection of professional secrecy, including medical confidentiality, in connection with this MSA.

6.2 Siemens Healthcare will Process Personal Data provided by the Institution as part of the provision of the Services. In contrast, Siemens will not Process Personal Data provided by the Institution. Siemens waives any right or title or interest it may have to Process such Personal Data unless the Institution permits Siemens to Process such Personal Data, in which case the Institution and Siemens will have to enter into an appropriate contract or other legal act under Union or Member State law in accordance with applicable data protection law.

6.3 Siemens does not make any warranties or representations regarding any Data provided or made available by any Individual User on teamplay or on any external website linked to it. Siemens does not warrant or represent that any such Data is true or accurate, or that it fulfils or serves any particular purpose.

6.4 The Institution shall report to Siemens any activities of any other user of teamplay which violate applicable laws and/or any of these terms.

7. Ownership; Third Party Licenses; Use Rights; Feedback

7.1 Siemens Healthcare and/or its licensors own all legal right, title and interest in and to the Services, and any software provided to the Institution as a part of and/or in connection with teamplay ("Software"), including any and all intellectual property rights that exist therein, whether registered or not, and wherever in the world they may exist. The Services and Software contain proprietary and confidential information that is protected by applicable

5. Подписки

5.1. Компания «Сименс» предлагает различные варианты Подписок. Базовая и Пробная подписки предоставляются бесплатно с возможностью перехода на Платную подписку с премиум-пакетами или дополнительными функциями, которые предлагаются за дополнительную плату. Пожалуйста, свяжитесь с торговыми представителями компании «Сименс» по вопросу Платной подписки.

5.2. По запросу компания «Сименс» предложит услуги по установке и/или конфигурации, которые оплачиваются Учреждением. Поддержка, оказываемая компанией «Сименс» в отношении Получателя, платформы teamplay и Базы данных, зависит от типа Подписки.

6. Ответственность за Персональные данные

6.1. Некоторые Данные, предоставляемые Учреждением, могут квалифицироваться как Персональные данные в соответствии с Законом Республики Казахстан № 94-V от 21 мая 2013 года «О персональных данных и их защите». В связи с этим Учреждение обязуется выполнять свои обязательства в качестве Контролера в соответствии со всеми действующими местными законами и положениями и/или законами и положениями по защите данных Европейского Союза, а также в соответствии со всеми действующими профессиональными и уголовными законодательными требованиями по защите профессиональной тайны, включая врачебную тайну, в рамках настоящего ГСПУ.

6.2. Компания «Сименс Здоровоохранение» Обработает Персональные данные, предоставленные Учреждением в рамках предоставления Услуг. А компания «Сименс», напротив, не будет Обрабатывать Персональные данные, предоставленные Учреждением. Компания «Сименс» отказывается от любых прав или интереса в отношении Обработки таких Персональных данных, кроме случаев, когда Учреждение разрешает компании «Сименс» Обрабатывать такие Персональные данные, и тогда Учреждение и компания «Сименс» должны будут заключить соответствующий контракт или другой законный акт согласно закону ЕС или страны-члена в соответствии с действующим законом по защите данных.

6.3. Компания «Сименс» не дает никаких гарантий и не делает никаких заявлений в отношении любых Данных, предоставленных Отдельным пользователем на платформе teamplay или любом подключенном внешнем веб-сайте. Компания «Сименс» не гарантирует и не заявляет, что такие Данные являются правдивыми и точными или что они служат какой-то конкретной цели либо выполняют какую-либо функцию.

6.4. Учреждение обязуется сообщать компании «Сименс» о действиях любого другого пользователя платформы teamplay, которые нарушают действующее законодательство и/или любые из настоящих условий.

7. Права собственности, сторонние лицензии, право пользования, обратная связь

7.1. Компания «Сименс Здоровоохранение» и/или ее лицензиары обладают всеми юридическими правами на Услуги и любое программное обеспечение, предоставленное Учреждению в рамках платформы teamplay и/или в связи с ней (далее — «Программное обеспечение»), включая все сопутствующие права на интеллектуальную собственность, как зарегистрированные, так и не зарегистрированные, вне зависимости от места их

intellectual property and other laws. Neither the Institution nor any third party shall obtain any express or implied rights in or to any part of the Software.

7.2 The use of teamplay may be subject to further license conditions for software that may be required by licensors of Siemens Healthcare. Siemens will make such additional license conditions available upon request. All title and interest to any such software shall remain with the licensors.

7.3 For the avoidance of doubt, Siemens and Siemens Healthcare do not claim ownership of Personal Data submitted or made available by the Institution or Individual Users. The Institution hereby grants to Siemens Healthcare the perpetual, non-exclusive, worldwide, irrevocable, royalty-free, unlimited, transferable and sublicensable right to use, import, modify, copy, transmit, display, reproduce, sublicense, aggregate, compile, decompile, manipulate, supplement, adapt, translate and create derivative works of the Network Data.

7.4 In the event the Institution, in connection with any of the Services, communicates suggestions for improvements relating to teamplay ("Feedback"), Siemens and Siemens Healthcare shall be entitled to use Feedback in its discretion and without restriction.

8. Term and Termination

8.1 Each Institution Account and the term of the MSA shall begin as of the date when the Institution Account is activated by Siemens or Siemens Healthcare and shall remain in full force and effect for an unlimited period of time but only as long as and to the extent the MSA entitles the Institution to permit its Individual Users to use teamplay and as long as at least a Basic Subscription is activated. An active Institution Account is required to affiliate with Individual Users. Each affiliated Individual User shall register for an user account which may be terminated by the Individual User at any time without cause by providing notice. Siemens may terminate each User Account without cause by giving thirty (30) days written notice.

8.2 Siemens may terminate the Institution's Account or parts of the Services with immediate effect upon notice in case of a material breach of this MSA by the Institution or its Individual Users that is not cured within thirty (30) days' notice of such breach. In addition, Siemens shall be entitled to cause Siemens Healthcare to delete Data posted or submitted by the Institution (respectively its Individual Users), issue a warning, and/or block access to teamplay until such material breach is cured.

нахождения. Услуги и Программное обеспечение содержат коммерческую и конфиденциальную информацию, которая защищена действующими законами о защите прав интеллектуальной собственности и другими законами. Ни Учреждение, ни какая-либо третья сторона не получит никаких явно выраженных или подразумеваемых прав ни на какую часть Программного обеспечения.

7.2. Использование платформы teamplay может подчиняться другим лицензионным условиям программного обеспечения, которые могут требоваться лицензиарами компании «Сименс Здоровоохранение». Компания «Сименс» предоставит такие дополнительные лицензионные условия по запросу. Все права на такое программное обеспечение останутся у лицензиаров.

7.3. Во избежание сомнений, компании «Сименс» и «Сименс Здоровоохранение» не будут претендовать на право собственности на Персональные данные, предоставленные Учреждением или Отдельными пользователями. Учреждение настоящим предоставляет компании «Сименс Здоровоохранение» бессрочное, неисключительное, всемирное, безотзывное, не требующее лицензионных отчислений, неограниченное, передаваемое и sublicензируемое право на использование, импорт, изменение, копирование, передачу, демонстрацию, воспроизведение, sublicензирование, объединение, компиляцию, декомпиляцию, манипуляцию, дополнение, адаптацию, перевод и создание производных работ из Сетевых данных.

7.4. Если Учреждение в связи с Услугами внесет предложения по улучшению платформы teamplay (далее «Обратная связь»), то компании «Сименс» и «Сименс Здоровоохранение» будут иметь право использовать такую Обратную связь без ограничений по своему усмотрению.

8. Срок действия и аннулирование

8.1. Каждая Учетная запись Учреждения и настоящее ГСПУ начнут действовать с даты активации Учетной записи Учреждения компанией «Сименс» или «Сименс Здоровоохранение» и останутся в силе на неопределенный период времени, но не более срока, на который настоящее ГСПУ дает право Учреждению разрешать своим Отдельным пользователям использовать платформу teamplay, и на период активации как минимум Базовой подписки. Активная Учетная запись Учреждения требуется для присоединения Отдельных пользователей. Каждый принятый Отдельный пользователь обязан зарегистрировать пользовательскую учетную запись, которая может быть аннулирована Отдельным пользователем в любое время без объяснения причин по предоставлению уведомления. Компания «Сименс» может аннулировать любую Учетную запись без объяснения причин, предоставив уведомление об этом за 30 (тридцать) дней.

8.2. Компания «Сименс» может аннулировать Учетную запись Учреждения или прекратить оказание части Услуг с немедленным вступлением в действие после предоставления уведомления, если Учреждение или его Отдельные пользователи значительно нарушили положения настоящего ГСПУ и это нарушение не было исправлено в течение 30 (тридцати) дней после предоставления уведомления о таком нарушении. Кроме того, компания «Сименс» вправе обязать компанию «Сименс Здоровоохранение» удалить Данные, опубликованные или предоставленные Учреждением (и, соответственно, его Отдельными пользователями), предоставить предупреждение и/или заблокировать

8.3 Siemens may also terminate the Institution's Account or (parts of) the Services with immediate effect upon notice (a) if any of the Services is not in conformity with applicable laws and legal conformity cannot be ensured within a reasonable time, or the establishment of such conformity would be unduly burdensome or otherwise unlawful for Siemens, or (b) in order to comply with applicable law or requests of governmental entities, or (c) if Siemens' or Siemens Healthcare' relationship with a third party who provides services or any other technology necessary to provide teamplay to the Institution expires, terminates or requires Siemens to change the way of use of such services or other technology as part of teamplay provided Siemens provides at least thirty (30) days' notice or similar means of communication in such event to the extent possible and, if such notice is not possible, to the extent Siemens provides as much notice or similar means of communication as possible under the circumstances, or (d) Siemens is no longer able to provide the Services due to circumstances beyond Siemens' reasonable control, or (e) if Siemens has decided to suspend or no longer offer teamplay by providing at least three (3) months prior notice.

8.4 Upon termination of the Institution's Account, Siemens shall be relieved of any obligations to grant access to teamplay and to provide any Services.

8.5 In the event of a legitimate termination for good cause attributable to Siemens or termination by Siemens according to section 8.3, the Institution shall be entitled to reimbursement of any prepaid fees covering the remainder of the term of the Institution's Account after the effective date of termination or unused portions of the Institution's Paid Subscription(s). For the avoidance of doubt, in case of termination in accordance with sections 8.1 or 8.2, the Institution shall not be entitled to claim reimbursement of any advance payments.

9. Modifications

9.1 Siemens may restrict, alter or reduce the Services, or modify this MSA at any time by providing a revised version of the MSA ("Revised Terms") in accordance with section 9.2 below.

9.2 Siemens will give the Institution at least six (6) weeks' notice of any material modification of the respective terms by sending an email or by giving notice in the teamplay application. In case of a material modification, the Institution shall be entitled to terminate its Institution Account or the respective Paid Subscription within six (6) weeks following the Institution's receipt of notice of the Revised Terms.

доступ к платформе teamplay до тех пор, пока такое значительное нарушение не будет исправлено.

8.3. Компания «Сименс» может также аннулировать Учетную запись Учреждения или (частично) прекратить оказание Услуг с немедленным вступлением в силу после предоставления уведомления, (а) если какие-либо Услуги нарушают действующее законодательство и выполнение требований законодательства невозможно обеспечить в разумные сроки, или обеспечение такого соответствия будет неоправданно сложным или незаконным для компании «Сименс»; или (б) для выполнения требований действующего законодательства или государственных органов; или (в) если отношения компании «Сименс» или «Сименс Здоровоохранение» с третьей стороной, которая предоставляет услуги или любые другие технологии, необходимые для предоставления Учреждению платформы teamplay, заканчивают свое действие, аннулируются или требуют, чтобы компания «Сименс» изменила способ использования таких услуг или других технологий в рамках платформы teamplay, при условии, что компания «Сименс» не менее чем за 30 (тридцать) дней предоставит уведомление или аналогичное средство коммуникации, насколько это возможно в такой ситуации, а если такое уведомление невозможно предоставить, то компания Сименс предоставит уведомление или аналогичное средство коммуникации как это будет возможно при сложившихся обстоятельствах; или (г) если компания «Сименс» не может больше предоставлять Услуги в результате обстоятельств, которые находятся вне разумного контроля компании «Сименс» не может оказать влияние; или (е) если компания «Сименс» решила приостановить или больше не предлагать платформу teamplay, направив предварительное уведомление не менее чем за 3 (три) месяца.

8.4. После аннулирования Учетной записи Учреждения компания «Сименс» будет освобождена от обязательства по предоставлению доступа к платформе teamplay и оказанию каких-либо Услуг.

8.5. В случае законного аннулирования по веской причине со стороны компании «Сименс» или аннулирования компанией «Сименс» в соответствии с разделом 8.3 Учреждение будет иметь право на получение компенсации любой суммы, уплаченной авансом за оставшийся период действия Учетной записи Учреждения после даты аннулирования, или неиспользованных частей Платной подписки (-ок) Учреждения. Во избежание сомнений в случае аннулирования в соответствии с условиями разделов 8.1 или 8.2 Учреждение будет не вправе требовать компенсацию любых сумм, уплаченных авансом.

9. Внесение изменений

9.1. Компания «Сименс» может ограничить, изменить или сократить Услуги либо внести изменения в настоящее ГСПУ (далее «Измененные условия») в соответствии с разделом 9.2 ниже.

9.2. Компания «Сименс» предоставит Учреждению уведомление о внесении любых существенных изменений в соответствующие условия не менее чем за 6 (шесть) недель по электронной почте или направив уведомление в приложении teamplay. В случае внесения существенных изменений Учреждение будет вправе аннулировать Учетную запись Учреждения или Платную подписку в течение 6 (шести) недель после получения Учреждением уведомления об Измененных условиях.

9.3 Non-material modifications will be performed subject to Siemens' discretion and will be accessible by following a respective link in the teamplay application.

9.3. Несущественные изменения будут вноситься по усмотрению компании «Сименс» и будут доступны по ссылке в приложении teamplay.

10. Data Backup; Uptime

TEAMPLAY IS NOT DEVELOPED FOR DATA BACKUP AND DOES NOT SUBSTITUTE ANY BACKUP OR STORAGE SYSTEM FOR ELECTRONIC OR HEALTH DATA. IT IS WITHIN THE INSTITUTION'S RESPONSIBILITY TO KEEP BACKUPS OF ANY AND ALL OF THE INSTITUTION'S DATA INCLUDING PERSONAL DATA.

It is technically impossible to achieve 100% availability of teamplay and the Receiver. In particular, Siemens shall not be responsible or liable, directly or indirectly, for any unavailability of teamplay or the Receiver caused by circumstances beyond Siemens' reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Siemens employees), or internet or cloud service provider failures or delays. In the event of planned downtimes, Siemens will provide prior notice as soon as reasonably feasible.

11. Limitation of Liability

11.1 Siemens' liability for damages caused by slight negligence, irrespective of its legal ground, shall be limited as follows:

- a. Siemens shall be liable up to the amount of the foreseeable damages typical for this type of contract due to a breach of material contractual obligations;
- b. Siemens shall not be liable due to a slightly negligent breach of any other duty of care applicable.

11.2 The aforesaid limitations of liability shall not apply to any mandatory statutory liability, in particular to liability for culpably caused injuries of life, body or health. In addition, such limitations of liability shall not apply if and to the extent Siemens has assumed a specific guarantee.

11.3 Sections 11.1 and 11.2 shall apply accordingly to Siemens' liability for futile expenses.

11.4 The Institution shall be obliged to take adequate measures to avert and reduce damages.

12. No Warranties

SIEMENS MAKES NO WARRANTIES, GUARANTEES OR REPRESENTATIONS OF ANY KIND, EXPRESS OR

10. Резервное копирование данных, время безотказной работы

ПРИЛОЖЕНИЕ TEAMPLAY НЕ ПРЕДНАЗНАЧЕНО ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ И НЕ ЗАМЕНЯЕТ СИСТЕМУ РЕЗЕРВНОГО КОПИРОВАНИЯ ИЛИ ХРАНЕНИЯ ЭЛЕКТРОННЫХ ИЛИ МЕДИЦИНСКИХ ДАННЫХ. ХРАНЕНИЕ РЕЗЕРВНЫХ КОПИЙ ВСЕХ ДАННЫХ УЧРЕЖДЕНИЯ, ВКЛЮЧАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ЯВЛЯЕТСЯ ОТВЕТСТВЕННОСТЬЮ УЧРЕЖДЕНИЯ.

Технически невозможно обеспечить 100-процентную доступность платформы teamplay и Получателя. В частности, компания «Сименс» не несет ответственности напрямую или косвенно за любое отсутствие доступа к платформе teamplay или Получателю по причине обстоятельств, на которые компания «Сименс» не может оказать разумного влияния, включая без ограничения стихийные бедствия, правительственные действия, наводнение, пожар, землетрясение, гражданские волнения, террористические акты, забастовки и другие трудовые проблемы (кроме тех, где задействованы сотрудники компании «Сименс»), а также за неполадки или задержки в работе поставщика Интернет-услуг или облачных услуг. В случае запланированных периодов работоспособности компания «Сименс» предоставит предварительное уведомление в кратчайшие разумные сроки.

11. Ограничение ответственности

11.1. Ответственность компании «Сименс» за ущерб, нанесенный в результате незначительной небрежности, вне зависимости от юридического основания ограничивается следующим:

- а) компания «Сименс» несет ответственность в рамках суммы прогнозируемого ущерба, типичного для такого рода соглашений, который произошел по причине нарушения существенных контрактных обязательств;
- б) компания «Сименс» не несет ответственности за незначительное нарушение любого другого применимого обязательства.

11.2. Вышеуказанные ограничения ответственности не применяются в отношении любой предусмотренной императивными нормами законодательства ответственности, в частности, в отношении ответственности за виновное причинение вреда жизни и здоровью. Кроме того, такие ограничения ответственности не применяются в случае и в пределах действия особой гарантии, которую предоставляет компания «Сименс».

11.3. Разделы 11.1 и 11.2 соответствующим образом применяются в отношении ответственности компании «Сименс» за нецелесообразные расходы.

11.4. Учреждение обязуется принять адекватные меры для предотвращения и сокращения размера ущерба.

12. Отсутствие гарантии

КОМПАНИЯ «СИМЕНС» НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ И НЕ ДЕЛАЕТ НИКАКИХ ЗАЯВЛЕНИЙ, ЯВНО

IMPLIED, WITH RESPECT TO THE OPERATION, CAPACITY, SPEED, FUNCTIONALITY, QUALIFICATIONS OR CAPABILITIES OF TEAMPLAY OR ANY GOODS OR PERSONNEL RESOURCES PROVIDED HEREUNDER, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT.

SIEMENS DOES NOT WARRANT ANY PARTICULAR RESULTS THAT MAY BE OBTAINED BY THE USE OF TEAMPLAY OR THAT THE SERVICES OR ASSOCIATED SYSTEMS WILL OPERATE IN AN ERROR-FREE OR UNINTERRUPTED MANNER, OR IN COMBINATION WITH THIRD PARTY PRODUCTS.

IN ANY CASE, THE INSTITUTION'S STATUTORY RIGHT TO REDUCE THE FEES SHALL BE EXCLUDED.

13. Notices

13.1 The Institution will receive all required notices electronically by using that email address. It is the Institution's responsibility to update or change its email address as appropriate.

13.2 Notices to the Institution will be provided by email or as notification within teamplay.

13.3 Unless otherwise stated, the Institution's notices to Siemens shall be send by email to support.teamplay.team@siemens-healthineers.com.

14. General Provisions

14.1 This Agreement shall be governed by the laws of the Republic of Kazakhstan excluding conflict of laws provisions.

14.2 Exclusive place of jurisdiction shall be court of the Republic of Kazakhstan.

14.3 The Institution may not assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of Siemens. Notwithstanding the foregoing, to the extent permitted by law, Siemens may assign rights and obligations relating to teamplay in whole or in part, without the Institution's consent, to its affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the Institution. Subject to the foregoing, this MSA shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

14.4 In case any of the provisions of this MSA shall be held to be invalid or unenforceable in any respect, the remaining provisions shall remain in full force and effect.

ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, В ОТНОШЕНИИ РАБОТЫ, МОЩНОСТИ, СКОРОСТИ, ФУНКЦИОНАЛЬНОСТИ, КВАЛИФИКАЦИЙ И ВОЗМОЖНОСТЕЙ ПЛАТФОРМЫ TEAMPLAY ИЛИ ЛЮБЫХ ПРОДУКТОВ И КАДРОВЫХ РЕСУРСОВ, ПРЕДОСТАВЛЕННЫХ В ЭТОЙ СВЯЗИ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЯ ЛЮБЫЕ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ В ОТНОШЕНИИ КОММЕРЧЕСКОЙ ПРИГОДНОСТИ ИЛИ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, ПРАВА СОБСТВЕННОСТИ ИЛИ ОТСУТСТВИЯ НАРУШЕНИЙ КАКИХ-ЛИБО ПРАВ.

КОМПАНИЯ «СИМЕНС» НЕ ГАРАНТИРУЕТ НИКАКИХ КОНКРЕТНЫХ РЕЗУЛЬТАТОВ, КОТОРЫЕ МОГУТ БЫТЬ ПОЛУЧЕНЫ ПРИ ИСПОЛЬЗОВАНИИ ПЛАТФОРМЫ TEAMPLAY, А ТАКЖЕ ТОГО, ЧТО УСЛУГИ ИЛИ СВЯЗАННЫЕ СИСТЕМЫ БУДУТ РАБОТАТЬ БЕЗОШИБОЧНО, НЕПРЕРЫВНО ИЛИ СОВМЕСТНО СО СТОРОННИМИ ПРОДУКТАМИ.

В ЛЮБОМ СЛУЧАЕ ПРЕДУСМОТРЕННОЕ ЗАКОНОМ ПРАВО УЧРЕЖДЕНИЯ НА СНИЖЕНИЕ ПЛАТЕЖЕЙ ИСКЛЮЧАЕТСЯ.

13. Уведомления

13.1. Учреждение будет получать необходимые уведомления в электронном виде по электронной почте. Учреждение несет ответственность за изменение или обновление адреса своей электронной почты.

13.2. Уведомления Учреждению будут направляться по электронной почте или предоставляться в рамках платформы teamplay.

13.3. Если не указано иное, уведомления Учреждения для компании «Сименс» должны отправляться по электронной почте на адрес support.teamplay.team@siemens-healthineers.com.

14. Общие положения

14.1. Настоящее Соглашение регулируется законодательством Республики Казахстан, за исключением положений о коллизионном праве.

14.2. Эксклюзивным местом рассмотрения споров является суды Республики Казахстан.

14.3. Учреждение не имеет права передавать какие-либо свои права или обязательства по настоящему соглашению в соответствии с законодательством или иным образом, не получив предварительное письменное согласие от компании «Сименс». Невзирая на вышеизложенное и при условии, что это не запрещено законодательством, компания «Сименс» может полностью или частично передавать свои права и обязательства, связанные с платформой teamplay, без согласия Учреждения своим аффилированным компаниям или в связи с поглощением, слиянием, реорганизацией или продажей всех или значительной части своих активов, где не задействован прямой конкурент Учреждения. С учетом вышеизложенного, настоящее ГСПУ будет иметь обязательную силу как для сторон, так и для их соответствующих наследников и разрешенных цессионариев.

14.4. Если какое-либо из положений настоящего ГСПУ станет незаконным или не имеющим исковой силы в любом отношении, то остальные положения будут полностью сохранять силу и действие.

License Schedule: Receiver Terms

1. Definitions

1.1 "Agreement" shall mean this license schedule.

1.2 "Licensed Software" shall mean the software program referred to as Receiver in Object Code format.

1.3 "Object Code" shall mean code for the Licensed Software resulting from translation of source code into machine readable format appropriate for execution by hardware.

2. License Grant

2.1 Subject to the terms of this Agreement, the Institution is granted for the term of this Agreement and subject to an active registration for teamplay, a non-exclusive, non-transferable license to use the Licensed Software for the Institution's operation of teamplay only in accordance with the MSA. The Institution acknowledges that it has no rights whatsoever in respect of the Licensed Software save for those expressly granted to it by this Agreement.

2.2 The Licensed Software may contain freeware, shareware or open source software. No license fee is charged to the Institution for the use of such freeware, shareware or open source software. Institution acknowledges and agrees that Siemens provides no warranties and shall have no liability whatsoever in respect of the Institution's possession and/or use of the freeware, shareware or open source software. Regarding such portions of Licensed Software, the Institution hereby accepts the specific license conditions ("Open Source Conditions"), which are available in the teamplay web application. Upon request of the Institution, Siemens will provide a copy of the source code of the open source software if required by the Open Source Conditions. To the extent there is a conflict between this Agreement and the Open Source Conditions, the terms of the Open Source Conditions shall prevail over the terms and conditions of this Agreement with regard to the open source software.

2.3 Certain programs of the Licensed Software may be proprietary to third party licensors who may be direct and intended third party beneficiaries of certain terms and conditions herein relating to the protection of such third party proprietary Licensed Software. The Institution agrees that those third party beneficiaries may enforce these terms and conditions directly against the Institution.

3. Copyright, Title

3.1 The Institution shall in any case use all reasonable efforts to safeguard the proprietary rights of right holders with regard to the Licensed Software.

3.2 The Institution shall not - and shall prevent others from doing so - copy, translate, modify, create derivative works, disassemble, reverse engineer, decompile, attempt, directly or indirectly, to otherwise obtain or create source

Лицензионное дополнение. Условия Получателя

1. Определения

1.1. «Соглашение» означает настоящее лицензионное дополнение.

1.2. «Лицензионное ПО» означает программное обеспечение, именуемое далее «Получатель» в формате Объектного кода.

1.3. «Объектный код» означает код для Лицензионного ПО, получаемый в результате перевода исходного кода в машинный формат, подходящий для использования аппаратными средствами.

2. Предоставление лицензии

2.1. В соответствии с условиями данного Соглашения, Учреждению на срок действия настоящего Соглашения и при условии действующей регистрации на платформе teamplay предоставляется неисключительная, непередаваемая лицензия на использование Лицензионного ПО только для работы Учреждения на платформе teamplay в соответствии с ГСПУ. Учреждение признает, что у него нет никаких прав на Лицензионное ПО, кроме тех, которые прямо предоставлены ему в рамках настоящего Соглашения.

2.2. Лицензионное ПО может содержать бесплатное ПО, условно-бесплатное ПО или ПО с открытым исходным кодом. Никакие лицензионные платежи не будут взиматься с Учреждения за использование такого бесплатного ПО, условно-бесплатного ПО или ПО с открытым исходным кодом. Учреждение соглашается с тем, что компания «Сименс» не предоставляет никаких гарантий и не несет ответственности за наличие у Учреждения или использование Учреждением такого бесплатного ПО, условно-бесплатного ПО или ПО с открытым исходным кодом. В отношении таких частей Лицензионного ПО Учреждение настоящим принимает специальные лицензионные условия (далее — «Условия открытого исходного кода»), которые приведены в приложении платформы teamplay. По запросу Учреждения компания «Сименс» предоставит копию исходного кода ПО с открытым исходным кодом, если это потребуется в соответствии с Условиями открытого исходного кода. В случае возникновения противоречий между настоящим Соглашением и Условиями открытого исходного кода, положения Условия открытого исходного кода будут иметь преимущественную силу над условиями настоящего Соглашения в отношении ПО с открытым исходным кодом.

2.3. Некоторые программы Лицензионного ПО могут принадлежать сторонним лицензиарам, которые могут являться прямыми сторонними бенефициарами некоторых условий данного Соглашения, связанных с защитой Лицензионного ПО таких сторонних владельцев. Учреждение соглашается с тем, что такие сторонние бенефициары могут обеспечить принудительное исполнение указанных условий Учреждением.

3. Авторское право, право собственности

3.1. Учреждение всегда будет прилагать все возможные усилия, чтобы защитить права правообладателей на Лицензионное ПО.

3.2. Учреждение не будет (и запретит другим лицам) копировать, переводить, изменять, создавать производные работы, разбирать, осуществлять обратное проектирование, декомпилировать, пытаться напрямую,

code of the Licensed Software for any reason other than as allowed under mandatory law or otherwise use the Licensed Software except as specifically authorized hereunder or by mandatory law.

3.3 The Institution agrees that using, distributing, copying, duplicating or otherwise reproducing all or any part of the Licensed Software other than in strict accordance with this Agreement, will be considered a material breach of this Agreement that is incapable of cure.

косвенно или иным образом получить или создать исходный код Лицензионного ПО по любой причине, кроме разрешенных императивными нормами закона случаев, либо иным образом использовать Лицензионное ПО, кроме случаев, четко указанных в настоящем Соглашении или предусмотренных действующими императивными нормами закона.

3.3. Учреждение согласно с тем, что использование, распространение, копирование, дублирование или иное воспроизведение всего или части Лицензионного ПО, кроме случаев, разрешенных настоящим Соглашением, будет считаться значительным нарушением настоящего Соглашения, которое невозможно исправить.

Annex 1: Data Processing Annex

This Data Processing Annex ("DPA") is entered into by and between the Institution ("Controller") and Siemens Healthcare GmbH, Henkestr. 127, 91052 Erlangen, Germany ("Processor"):

1.1 The Processor shall Process Personal Data provided by the Controller only on behalf of and only on documented instructions from the Controller in accordance with the Data Processing Agreement in Schedule 1 of this Data Processing Annex and in accordance with the Services provided under the MSA.

1.2 Capitalized terms used in this Data Processing Annex or in Schedule 1 shall have the meaning as defined in Section 0 of the MSA (including the definition of "MSA").

2.1 The Controller shall be responsible for any Personal Data posted, submitted or otherwise disclosed by it and/or its Individual Users and verification of the identity of any other user such Personal Data is shared with and/or transferred to.

2.2 Personal Data being Processed by the Receiver and/or uploaded to the cloud-deployed database will be stored in such database operated by Microsoft ("Database"). For this purpose, the Processor has entered into a sub-processing agreement with Microsoft Ireland Operations Limited, Ireland. Further, the Processing of the Personal Data is performed by the Processor and its sub-processor Siemens Healthcare Private Limited, India. Exceptionally for troubleshooting purposes, the Processor may (i) provide Microsoft Corporation, Redmond, USA, or its sub-processors with system data relating to support tickets or (ii) permit access to log data of Microsoft Azure Platform services, both of which may or may not include Personal Data.

In addition, the Processor and/or its affiliates may offer remote support services in connection with the Services and/or the Receiver. When using such remote support services, the Processor and/or its affiliates may get access to Data that contain Personal Data.

2.3 The Controller shall (and shall ensure that its Individual Users do) submit or otherwise disclose Personal Data to the Processor only to the extent there is a legal justification, i.e. the Controller has obtained prior voluntary informed consent from the individual concerned (a consent form can be provided on request) or the Institution can justify such submission by other valid legal ground for the processing of Personal Data in accordance with applicable law. If the Controller uses Receiver settings requiring such legal justification, the Controller is responsible to ensure such legal justification before changing the settings. If such legal justification does not exist, the Controller shall explicitly block the individuals concerned.

Приложение 1. Приложение об обработке данных

Настоящее Приложение об обработке данных (далее — «ПОД») заключается между Учреждением (далее — «Контролер») и компанией «Сименс Хелскэа ГмБХ», Henkestr. 127, 91052 Erlangen, Germany (Германия) (далее — «Обработчик»).

1.1. Обработчик обязуется Обрабатывать Персональные данные, предоставленные Контролером, только от имени и по документальным инструкциям Контролера, в соответствии с Соглашением по обработке данных в Дополнении 1 к настоящему Приложению об обработке данных и в соответствии с Услугами по настоящему ГСПУ.

1.2. Термины, написанные с заглавной буквы в настоящем Приложении об обработке данных или в Дополнении 1, имеют значение, которое определено в разделе 0 ГСПУ (включая определение «ГСПУ»).

2.1. Контролер несет ответственность за любые Персональные данные, опубликованные, поданные или иным образом раскрытые им и/или его Отдельными пользователями, а также за проверку личности любого другого пользователя, который получает доступ к таким Персональным данным и/или которому они передаются.

2.2. Персональные данные, Обрабатываемые Получателем и/или загруженные в базу данных на облачном сервисе, будут храниться в такой базе данных, которая управляется Microsoft (далее — «База данных»). Для этой цели Обработчик заключил соглашение о субобработке с компанией Microsoft Ireland Operations Limited, Ирландия. Кроме того, Обработка персональных данных осуществляется Обработчиком и его субобработчиком, компанией «Сименс Хелскэа Прайвит Лимитэд», Индия. Исключительно для целей устранения неполадок, Обработчик может (i) предоставить компании Microsoft Corporation, Редмонд, США, или ее субобработчикам системные данные, относящиеся к заявкам в службу поддержки или (ii) разрешить доступ к log-данным услуг платформы Microsoft Azure, при этом обе категории указанных данных могут как включать в себя, так и не включать Персональные данные.

Кроме того, Обработчик и/или его аффилированные компании могут предложить удаленную поддержку в связи с Услугами и/или Получателем. При использовании услуги удаленной поддержки Обработчик и/или его аффилированные компании могут получить доступ к Данным, которые содержат Персональные данные.

2.3. Контролер обязуется (и обеспечит выполнение этого требования Отдельными пользователями) предоставлять или иным образом раскрывать Персональные данные Обработчику только в том случае, если для этого есть юридическое обоснование, т.е. Контролер получил предварительное добровольное согласие от соответствующего физического лица (форма согласия может быть предоставлена по запросу) или Учреждение может обосновать такое предоставление другими законными основаниями для обработки Персональных данных в соответствии с действующим законодательством. Если Контролер использует настройки Получателя, требующие такого законного обоснования, то Контролер несет ответственность за обеспечение этого юридического обоснования до изменения настроек. Если указанного юридического обоснования нет, то Контролер обязуется четко блокировать таких задействованных физических лиц.

2.4 The Controller warrants that Personal Data disclosed to the Processor by the Controller and/or its Individual Users is Processed in accordance with applicable privacy, data protection and medical secrecy regulations and the Controller's notifications with the competent data protection authority, if any. The Controller warrants that the submission and disclosure as well as the further Processing of Data are permitted. This applies in particular to the extent Data submitted or otherwise disclosed by the Controller and/or its Individual Users on teamplay contains any protected Personal Data or any other sensitive or confidential information.

2.5 In order to fulfil its obligations under this section 2 the Controller will be able to change the privacy settings of the Receiver in accordance with its local (legal) requirements. Upon request of the relevant data subject or any person entitled, the Controller shall immediately cease using teamplay based on settings permitting the use of Personal Data of such data subject and block such Personal Data for Processing by the Receiver. The Controller is responsible for the settings of the Receiver required to fulfil the aforementioned obligations. The settings will provide for the possibility to either blacklist several patients or to put a tag into the DICOM data file within each study.

2.6 If Controller actively transmits Data to the Receiver or Database, this Section 2 applies accordingly and Controller shall anonymize such Data before sending, if Controller lacks a legal justification. This is of utmost importance for the use of the application "teamplay Images".

2.7 Older medical devices being connected via the DICOM nodes to the Receiver might submit Data required for the teamplay functionalities in the form of so called black images (i.e. as burned in information represented in a DICOM secondary capture image). In such cases the required information is directly scanned from the DICOM image via an embedded OCR scan in the Receiver. In order to perform such scan the black image needs to be of good image quality. If the image quality is poor the scan might either not be error-free or the Receiver might not be able to black-out the relevant information according to the settings before submitting the derived information to the Database. In such case, as well as in case the scanner is not correctly recognized, the Receiver may submit Personal Data to the Database despite the more restrictive settings.

2.8 Physicians, medical physicists and other healthcare professionals are bound by medical confidentiality. Therefore, when using teamplay, the Controller is responsible for (a) anonymization of patient data according to applicable laws and regulations or (b) obtaining patient's prior written release from medical confidentiality according to applicable laws and regulations, if required and to the extent admissible according to local laws.

2.9 The Controller shall be responsible for obtaining the consent of its employees or self-employed personnel for

2.4. Контролер гарантирует, что Персональные данные, раскрываемые Обработчику Контролером и/или его Отдельными пользователями, Обработываются в соответствии с действующими положениями о конфиденциальности, защите данных, врачебной тайне и уведомлениями Контролера от компетентных органов по защите данных, если таковые имеются. Контролер гарантирует, что предоставление и раскрытие, а также дальнейшая Обработка Данных разрешены. Это особенно относится к тем Данным, которые предоставлены или иным образом раскрыты Контролером и/или Отдельными пользователями на платформе teamplay и содержат любые защищенные Персональные данные либо любую другую конфиденциальную информацию или информацию с ограниченным доступом.

2.5. Для того чтобы выполнить свои обязательства, изложенные в разделе 2, Контролер сможет изменить настройки конфиденциальности Получателя в соответствии с местными (законными) требованиями. По запросу соответствующего субъекта данных или любого уполномоченного лица Контролер незамедлительно прекратит использование платформы teamplay на основании настроек, разрешающих использование Персональных данных такого субъекта данных, и заблокирует такие Персональные данные для Обработки Получателем. Контролер несет ответственность за настройки Получателя, требуемые для выполнения вышеуказанных обязательств. Настройки обеспечат возможность занести в черный список некоторых пациентов или проставить отметки в файле данных DICOM в рамках каждого исследования.

2.6. Если Контролер активно передает Данные Получателю или в Базу данных, то положения настоящего раздела 2 применяются соответствующим образом, и Контролер обязуется обезличить такие Данные перед отправлением, если у Контролера нет законного основания на это. Это очень важно при использовании приложения teamplay Images.

2.7. Более старые медицинские изделия, подключенные к Получателю через узлы DICOM, могут предоставлять Данные, требуемые для функций платформы teamplay, в форме так называемых черных изображений (т. е. как записано в информации, представленной во второстепенном образе захвата DICOM). В таких случаях требуемая информация напрямую сканируется из образа DICOM через встроенное в Получатель оптическое читающее устройство. Для проведения такого сканирования черное изображение должно быть хорошего качества. При плохом качестве изображения сканирование может пройти с ошибками или Получатель может не суметь скрыть необходимую информацию в соответствии с настройками до подачи извлеченной информации в Базу данных. В таком случае, а также в случае некорректного распознавания сканнером Получатель может отправить Персональные данные в Базу данных, не взирая на более ограничивающие настройки.

2.8. Врачи, медицинские физики и другие медицинские сотрудники обязаны сохранять врачебную тайну. Поэтому при использовании платформы teamplay Контролер несет ответственность (а) за обезличивание данных пациента в соответствии с действующими законами и иными нормативно-правовыми актами или (б) получение предварительного письменного отказа пациента от врачебной тайны в соответствии с действующими законами и иными нормативно-правовыми актами, если это необходимо и в пределах, допустимых местным законодательством.

2.9. Контролер несет ответственность за получение согласия своих сотрудников или самозанятых

the Processing of Data containing information on employees (especially physicians and operators). The settings of the Receiver provide for the possibility to exclude Data containing information about such employees.

2.10 The Processor and the Controller shall co-operate with each other to promptly and effectively handle and solve enquiries, complaints, and claims relating to the Processing of Personal Data from any court, government official (including but not limited to any data protection or law enforcement agency), third parties or individuals (including but not limited to requests of the data subjects to access, rectify, erase or block Personal Data concerning them).

2.11 To the extent Services provide functionality to request the disclosure or submission of Data to Third-Party Solutions operated by Third-Party Providers (such as a "Open with/Open in/Send to"- functionality), the Controller hereby instructs the Processor to disclose or submit the Data to the Third-Party Provider upon such request only. The Controller is only entitled to use such functionality if Controller has entered into a data processing agreement with such Third-Party Provider and ensures the legal justification to submit or disclose Data to such Third-Party Provider. The Processor only follows the foregoing instruction and is thereby not acting as a sub-processor to such Third-Party Provider.

2.12 The Controller shall be responsible for initial collection, recording, systematisation, storing, updating, amending, transferring and extraction (collectively "Initial Processing") of the Personal Data. The Controller hereby represents that it can organize Initial Processing of the Personal Data in compliance with laws governing processing and protection of such information, particularly, the Controller represents that it has obtained the individuals' consent on the transfer (including consent/information about cross-boundary transfer) of their Personal Data to the Processor and back to the Controller, and processing of the Personal Data by the Controller. The Controller shall not be allowed to transfer Personal Data to the Processor, if it has not done the Initial Processing in compliance with laws.

сотрудников на Обработку данных, содержащих информацию о сотрудниках (особенно врачах и операторах). Настройки Получателя дают возможность исключать Данные, содержащие информацию о таких сотрудниках.

2.10. Обработчик и Контролер должны сотрудничать друг с другом в целях быстрой и эффективной обработки и решения запросов, претензий и требований, связанных с Обработкой Персональных данных, получаемых из судов, от государственных должностных лиц (включая без ограничения любые органы по защите данных и правоохранительные органы), третьих лиц или физических лиц (включая без ограничения запросы субъектов данных на доступ, исправление, удаление или блокирование Персональных данных, связанных с ними).

2.11. В тех случаях, когда Услуги предоставляют функцию запроса на раскрытие или подачу Данных Сторонним решениям, которые контролируются Сторонними провайдерами (как, например, функция «Открыть с помощью/открыть в/отправить»), Контролер настоящим предписывает Обработчику раскрывать и подавать эти Данные Стороннему провайдеру только по такому запросу. Контролер имеет право использовать эту функцию, только если он заключил соглашение по обработке данных с таким Сторонним провайдером и гарантирует наличие юридического обоснования для подачи или раскрытия Данных такому Стороннему провайдеру. Обработчик только выполняет вышеуказанные предписания и не выступает в качестве субобработчика для такого Стороннего провайдера.

2.12. Контролер несет ответственность за сбор, запись, систематизацию, хранение, обновление, изменение, передачу и удаление (совместно - «Первичная обработка») Персональных данных. Настоящим Контролер заверяет и гарантирует, что осуществляет Первичную обработку Персональных данных в соответствии с нормами законодательства, регулирующими обработку и защиту такой информации, в частности, Контролер заверяет, что получил согласие физических лиц на передачу (в том числе, согласие / информирование о трансграничной передаче) Персональных данных Обработчику и обратно Контролеру, и обработку Обработчиком Персональных данных. Контролер не должен каким-либо образом передавать Обработчику такие данные, если не произвел Первичную обработку Персональных данных в соответствии с законодательством.

Schedule 1: Data Processing Agreement

Дополнение 1. Соглашение об обработке данных

Article 1 Subject-matter, nature, purpose and duration of the processing

- (1) This Schedule 1 supplements the DPA. It applies to the Processing of Personal Data by Processor on behalf of the Controller under the DPA and sets out the data protection obligations of the parties.
- (2) Nature and purpose of Processing: Processor Processes Personal Data to the extent necessary to provide the Services specified and agreed in the MSA.
- (3) Processor and Controller are each responsible for their own compliance with the applicable data protection law. The Controller is solely responsible for the means by which the Processor acquired the Personal Data and the Controller shall only disclose Personal Data to the Processor for which a legal authorization is given and for which the Controller has a legal right of Processing.
- (4) The duration of the Processing corresponds to the term of the MSA.

Article 2 Type of Personal Data and categories of data subjects

The types of Personal Data and categories of data subjects are laid out in **Attachment 1**.

Article 3 Instructions

- (1) The Processor Processes Personal Data only on the basis of the Controller's documented instructions. The DPA and the MSA are the Controller's complete and final documented instructions to Processor for the Processing of Personal Data.
- (2) Any additional or alternate instructions (in particular Section 2.11 of the DPA) must be issued by the Controller in writing and are binding only upon written acknowledgement by Processor. Processor shall inform the Controller if, in Processor's opinion, an instruction infringes the GDPR or the data protection provisions applicable to Processor. Processor is under no obligation to conduct a comprehensive legal review or to follow instructions prohibited by law.
- (3) The Controller shall bear all additional costs incurred by Processor as a result of an additional or alternate instruction, unless the instruction is necessary to comply with statutory requirements applicable to Processor.

Article 4 Confidentiality

Раздел 1. Предмет, характер, назначение и срок обработки

- (1) Настоящее дополнение 1 дополняет ПОД. Оно действует в отношении Обработки Персональных данных Обработчиком от имени Контролера согласно ПОД и излагает обязательства сторон по защите данных.
- (2) Характер и назначение Обработки: Обработчик Обрабатывает Персональные данные в объеме, необходимом для предоставления Услуг, указанных и согласованных в ГСПУ.
- (3) Обработчик и Контролер несут ответственность за соблюдение ими действующего законодательства по защите данных. Контролер единолично несет ответственность за средства, с помощью которых Обработчик получает Персональные данные, и Контролер может раскрывать Персональные данные только тому Обработчику, на которого получено юридическое разрешение и для которого Контролер имеет право проводить Обработку.
- (4) Длительность обработки соответствует сроку действия ГСПУ.

Раздел 2. Виды Персональных данных и категории субъектов данных

Виды Персональных данных и категории субъектов данных изложены во **Вложении 1**.

Раздел 3. Указания

- (1) Обработчик обрабатывает Персональные данные только на основании документальных указаний Контролера. ПОД и ГСПУ представляют собой полные и окончательные документальные указания Обработчику по Обработке Персональных данных.
- (2) Любые дополнительные или альтернативные указания (в частности, раздел 2.11 ПОД) должны предоставляться Контролером в письменном виде. Они являются обязательными только после письменного подтверждения со стороны Обработчика. Обработчик обязуется уведомить Контролера, если, по мнению Обработчика, указания нарушают Общий регламент по защите данных или положения по защите данных, применимые к Обработчику. Обработчик не обязан проводить комплексную юридическую проверку или выполнять указания, запрещенные законодательством.
- (3) Контролер обязуется компенсировать все дополнительные расходы, понесенные Обработчиком в результате выполнения дополнительных или измененных указаний, кроме случаев, когда такое указание необходимо выполнить для соблюдения законодательных требований, действующих в отношении Обработчика.

Раздел 4. Конфиденциальность

Processor warrants that persons authorized to Process the Personal Data are bound to continuing secrecy by contract or are under such a duty by law.

Обработчик гарантирует, что лица, уполномоченные проводить Обработку Персональных данных, обязаны выполнять требования о соблюдении постоянной конфиденциальности по контракту или такие же требования согласно законодательству.

Article 5 Security of Processing

- (1) Processor shall take all measures required pursuant to Article 32 GDPR.
- (2) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and in particular the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed, Processor shall implement technical and organizational measures as set out in **Attachment TOM**.
- (3) The Controller and Processor agree that the implementation of the technical and organizational measures described in **Attachment TOM** ensures an appropriate level of safety in accordance with the GDPR and provides sufficient safeguards for the protection of the rights of the data subject.
- (4) The technical and organizational measures described in **Attachment TOM** are subject to technical progress and further development and may be adjusted by Processor if appropriate, provided such adjustment does not result in a lower level of protection than that set forth in **Attachment TOM**.

Article 6 Sub-processors

- (1) Processor engages sub-processors (another processor) to carry out specific Processing activities on behalf of the Controller. Sub-processors are only allowed to Process Personal Data for the purpose of carrying out the activities for which such Personal Data have been provided to Processor and are prohibited from Processing Personal Data for other purposes. If Processor engages sub-processors, they will be subject to written data protection obligations, providing at least the same level of protection as set forth in this DPA.
- (2) The list of sub-processors currently engaged by Processor is detailed out in the DPA. Processor reserves the right to update this list by setting up an URL within teamplay.

The Controller hereby authorizes Processor to engage the listed companies as sub-processors. If available, the Controller shall subscribe to a Processor' website to receive the information regarding additional sub-processors and for any intended changes in the use or replacement of sub-processors.

Раздел 5. Конфиденциальность обработки

- (1) Обработчик обязуется принять все необходимые меры, требуемые в соответствии со статьей 32 Общего регламента по защите данных.
- (2) Принимая во внимание существующее положение дел, стоимость реализации, характер, объем, контекст и назначение Обработки, а также риск различной вероятности и строгости в отношении прав и свобод физических лиц, а именно риски, которые связаны с Обработкой, такие как случайное или незаконное уничтожение, потеря, изменение, несанкционированное раскрытие или доступ к Персональным данным, которые передаются, хранятся или иным образом обрабатываются, Обработчик обязан принимать технические и организационные меры, указанные в **Приложении TOM**.
- (3) Контролер и Обработчик согласны с тем, что реализация технических и организационных мер, указанных в **Приложении TOM**, гарантирует необходимый уровень безопасности в соответствии с положениями Общего регламента по защите данных и обеспечивает достаточные меры безопасности для защиты прав субъекта данных.
- (4) Технические и организационные меры, указанные в **Приложении TOM**, зависят от технического прогресса и дальнейшего развития, а также могут корректироваться Обработчиком, если это уместно, при условии, что такие корректировки не приведут к снижению уровня защиты, который указан в **Приложении TOM**.

Раздел 6. Субобработчики

- (1) Обработчик привлекает субобработчиков (другого обработчика) для проведения специальных видов деятельности, связанных с Обработкой, от имени Контролера. Субобработчикам разрешается Обрабатывать Персональные данные только с целью осуществления тех видов деятельности, для которых такие Персональные данные были предоставлены Обработчиком; им запрещается Обрабатывать Персональные данные для других целей. Если Обработчик привлекает субобработчиков, то они будут подчиняться письменным обязательствам по защите данных, которые обеспечивают как минимум такой же уровень защиты, который описан в настоящем ПОД.
- (2) Перечень субобработчиков, привлеченных на данный момент Обработчиком, приведен в ПОД. Обработчик оставляет за собой право обновлять этот перечень, указав ссылку на платформе teamplay.

Контролер настоящим разрешает Обработчику привлекать указанные компании в качестве субобработчиков. Если есть возможность, Контролер обязуется подписаться на веб-сайт Обработчика для получения информации о дополнительных субобработчиках и любых плановых изменениях в привлечении или замене субобработчиков.

- (3) The engagement or replacement of an additional sub-processor shall be deemed approved if Processor informs the Controller in advance thereof and the Controller raises no objection to Processor in writing, including in electronic form, within 3 months following such information.
- (4) If the Controller objects the Controller shall notify Processor in detail about the reasons for the objection.
- Following an objection, Processor may at its discretion
- propose another sub-processor in place of the rejected sub-processor; or
 - take steps to address the concerns raised by the Controller which remove the Controller's objection.
- (5) If the options as per this Article 6 (4) a. and b. are reasonably not available or the objection has not been removed otherwise, Processor may terminate the DPA in full or in part without notice, e.g. if the Controller's objection makes it considerably more difficult or impossible for Processor to perform its contractual obligations. Following the termination of the DPA by Processor Siemens may terminate the MSA.
- (6) Any agreements on response times or availability will be suspended and any claims in this regard for damages in lieu of performance, for delay or for any agreed liquidated damages or contractual penalties with regard to Processor do not apply from the planned start date of the objected to sub-processor onwards. If Processor' performance obligations are terminated in part, the remuneration for the Services unaffected by the partial termination shall be determined in accordance with Processor' standard list prices applicable to such services at Processor.
- (7) Where the sub-processor fails to meet its data protection obligations, Processor shall – in accordance with the provisions on liability in the MSA – remain fully liable to the Controller for the performance of the sub-processor's obligations. Processor shall not be liable for damages and claims arising from the Controller's additional or alternate instructions as per Article 3 (2) of this DPA.
- (8) In case Processor engages a sub-processor in a third country (outside the EU/EEA), Processor shall use data transfer mechanisms compliant with Article 44 et seq. GDPR. Processor shall in particular provide sufficient safeguards that the appropriate technical and organizational measures are implemented in such a way that Processing meets the requirements of the GDPR, ensure the protection of the rights of the data subjects concerned, maintain a record of data transfers and document suitable safeguards.
- (3) Привлечение и замена дополнительных субобработчиков будет считаться одобренной, если Обработчик заранее сообщит Контролеру о таком событии и Контролер не выскажет никаких возражений Обработчику в письменном виде или в электронной форме в течение 3 месяцев после предоставления такой информации.
- (4) Если Контролер возражает, то он обязуется уведомить Обработчика о причинах такого возражения.
- После предоставления возражения Обработчик может по своему усмотрению:
- предложить другого субобработчика вместо отклоненного или
 - предпринять меры для разрешения вопросов, поднятых Контролером, которые снимут такие возражения.
- (5) Если варианты, указанные в разделе 6 (4) а и б, обоснованно не могут быть использованы или такие возражения не были устранены другим способом, то Обработчик может аннулировать данное ПОД полностью или частично без предоставления уведомления, например, если возражения Контролера значительно усложняют или делают невозможным выполнение Обработчиком своих контрактных обязательств. После аннулирования Обработчиком ПОД компания «Сименс» может расторгнуть ГСПУ.
- (6) Любые договоренности о времени отклика или доступности будут приостановлены, и любые требования в этой связи относительно ущерба, просрочки, согласованных и заранее оцененных убытков или договорных штрафов в отношении Обработчика не будут применяться с планируемой даты выдвигения возражений субобработчику. Если обязательства Обработчика аннулированы частично, то вознаграждение за Услуги, не затронутые частичным аннулированием, будет определяться в соответствии со стандартным прейскурантом Обработчика, действующим в отношении таких услуг.
- (7) Если субобработчик не выполнит своих обязательств по защите данных, то Обработчик обязуется, в соответствии с положениями об обязательствах в ГСПУ, нести полную ответственность перед Контролером за выполнение обязательств субобработчика. Обработчик не несет ответственности за ущерб и требования, возникающие в связи с дополнительными или измененными указаниями Контролера в соответствии с разделом 3 (2) данного ПОД.
- (8) Если Обработчик привлечет субобработчика в третьей стране (за пределами ЕС/Европейской экономической зоны), то Обработчик обязуется использовать механизмы передачи данных в соответствии со статьей 44 и последующими статьями Общего регламента по защите данных. Обработчик обязуется обеспечить достаточные меры безопасности, чтобы необходимые технические и организационные меры были реализованы таким образом, чтобы Обработка соответствовала требованиям Общего регламента по защите данных, а также гарантировать защиту прав соответствующих субъектов данных, вести

регистрацию передачи данных и документировать подходящие меры безопасности.

- (9) In case Processor provides sufficient safeguards e.g. by standard contractual clauses according to EU Commission decision 2010/87/EU or standard protection clauses according to Article 46 ("standard data protection clauses"), the Controller herewith grants power of attorney to Processor to enter into such standard data protection clauses in the name and for the account of the Controller. Further, the Controller expressly permits Processor to also represent the respective sub-processor when entering into such standard data protection clauses. This means that Processor is entitled to act on behalf of the Controller and the sub-processor. Processor is also entitled to exercise the Controller's rights and powers under the standard data protection clauses vis-à-vis the sub-processor.

- (9) Если Обработчик обеспечит достаточные меры безопасности, например, по стандартным контрактным условиям в соответствии с решением Комиссии ЕС 2010/87/EU или по стандартным условиям по защите в соответствии со статьей 46 (далее «стандартные условия по защите данных»), то Контролер настоящим предоставляет полномочия Обработчику заключать такие стандартные условия по защите данных от имени и за счет Контролера. Кроме того, Контролер также разрешает Обработчику представлять соответствующего субобработчика при заключении таких стандартных условий по защите данных. Это означает, что Обработчик имеет право действовать от имени Контролера и субобработчика. Обработчик также имеет право использовать права и полномочия Контролера по стандартным условиям касательно защиты данных в отношении субобработчика.

Article 7 Assistance

- (1) Taking into account the nature of the Processing as described in the MSA and this DPA, Processor will assist the Controller upon request and at the Controller's expense by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Articles 12 to 23 GDPR.
- (2) Processor shall inform the Controller without undue delay about requests from data subjects to exercise their rights as per Articles 12 to 23 GDPR, in particular with regard to the right of access to Personal Data, right to rectification, right to erasure ('right to be forgotten'), right to restriction of Processing, right to data portability, right to object or the right not to be subject to an automated individual decision-making.
- (3) Taking into account the nature of the Processing as described in the MSA and this DPA and the information available at Processor, Processor shall assist the Controller at the Controller's expense in ensuring Controller's own compliance with the obligations pursuant to Articles 32 (security of Processing), 33 (notification of Personal Data breach to the supervisory authority), 34 (communication of a Personal Data breach to the data subject), 35 (data protection impact assessment) and 36 (prior consultation) GDPR.

Article 8 Deletion

At the choice of the Controller all Personal Data of the Controller are to be deleted or returned after the end of the provision of Services relating to Processing. Controller hereby instructs Processor to delete all Personal Data of the Controller after the end of the provision of Services relating to Processing and to

Раздел 7. Оказание помощи

- (1) Принимая во внимание характер Обработки, описанный в ГСПУ и настоящем ПОД, Обработчик будет оказывать помощь Контролеру по запросу и за счет Контролера соответствующими техническими и организационными мерами, насколько это возможно, для выполнения обязательств Контролера по ответу на запросы относительно использования прав субъекта данных, изложенных в статьях с 12 по 23 Общего регламента по защите данных.
- (2) Обработчик обязуется незамедлительно сообщить Контролеру о запросах от субъектов данных об осуществлении их прав согласно статьям 12–23 Общего регламента по защите данных, в частности, относительно права доступа к Персональным данным, права на внесение поправок, права на удаление данных («право на забвение»), право на ограничение Обработки, право на перенос данных, право на возражение или право не подвергаться индивидуальной автоматической процедуре принятия решения.
- (3) Принимая во внимание характер Обработки, описанный в ГСПУ и ПОД, а также в информации, имеющейся у Обработчика, Обработчик обязан оказать помощь Контролеру за его счет в обеспечении выполнения Контролером своих обязательств согласно статьям 32 (безопасность Обработки), 33 (уведомление контролирующего органа о нарушении, связанном с Персональными данными), 34 (уведомление субъекта данных о нарушении, связанном с Персональными данными), 35 (оценка влияния защиты данных) и 36 (предварительная консультация) Общего регламента по защите данных.

Раздел 8. Удаление

По усмотрению Контролера все Персональные данные Контролера должны удаляться или возвращаться после окончания предоставления Услуг, связанных с Обработкой. Контролер настоящим предписывает Обработчику удалить все Персональные данные Контролера после окончания

delete existing copies unless Union or Member State law requires storage of the Personal Data.

предоставления Услуг, связанных с Обработкой, и удалить существующие копии, кроме случаев, когда законодательство ЕС или страны-члена ЕС требует хранить такие Персональные данные.

Article 9 Information and audit rights

- (1) With regard to the Processing under the MSA and the DPA, Processor shall upon the Controller's written request make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.
- (2) Processor shall allow for and contribute to Controller audits, including inspections ("audits"), with regard to the Processing under the main contract to demonstrate compliance with the obligations laid down in Article 28 GDPR. These audits may also be conducted by an independent third party auditor mandated by the Controller, provided that this auditor is acceptable for Processor and bound by confidentiality. The Controller shall request an audit with reasonable prior notice to Processor. Prior to an audit, the parties shall mutually agree on the scope, timing, and duration of the audit. The Controller shall reimburse Processor for any services incurred by Processor with regard to the audit at the then current Processor service rates, which shall be made available to the Controller upon request.
- (3) The Controller shall promptly provide a written report to Processor containing a confidential summary of the scope and results of the audit. Irrespective hereof, Processor is entitled to use the report for its own purposes.

Раздел 9. Права на информацию и аудит

- (1) В отношении Обработки согласно ГСПУ и ПОД Обработчик обязан по письменному запросу Контролера предоставить Контролеру всю информацию, которая необходима для подтверждения выполнения обязательств, изложенных в статье 28 Общего регламента по защите данных.
- (2) Обработчик разрешит и будет способствовать проведению аудита Контролером, включая проверки (далее — «аудит»), относительно Обработки по основному соглашению для подтверждения выполнения обязательств, указанных в статье 28 ГСПУ. Такие аудиты могут также проводиться независимым сторонним аудитором, назначенным Контролером, при условии, что такой аудитор приемлем для Обработчика и связан обязательствами по соблюдению конфиденциальности. Контролер запрашивает аудит, заблаговременно предоставив Обработчику уведомление в письменном виде. До проведения аудита стороны согласуют объем, время и продолжительность аудита. Контролер обязуется компенсировать Обработчику любые расходы на услуги, понесенные Обработчиком в связи с проведением аудита, по ставкам на услуги, действующим у Обработчика на момент проведения аудита, которые будут предоставлены Контролеру по запросу.
- (3) Контролер обязуется незамедлительно предоставить Обработчику письменный отчет, содержащий краткие конфиденциальные данные об объеме и результатах такого аудита. Обработчик имеет право использовать такой отчет для своих целей.

Attachment 1
Details of the Transfer

Categories of data subjects: The Personal Data transferred concern the following categories of data subjects:

- Employees or suppliers of the Controller or the Controller's group companies
- Patients of the Controller or the Controller's group companies

Types of Personal Data: The Personal Data transferred concern the following categories of data:

Employee data, supplier data or data related to the Controller, such as business contact information (e.g. name, work address, work phone number, work email address, work mobile phone number, job title).

- Patient data, such as patient related information (e.g. DICOM attributes, DICOM images/pixel data).

Special categories of data: The Personal Data transferred concern the following special categories of data:

- Data on health, biometrical data

Processing operations: The Personal Data transferred will be subject to the following basic Processing activities:

The type, subject matter of the Processing, nature and purpose of the Processing of Personal Data are further specified in the MSA between the Controller and Siemens Healthcare LLC, Khadzhy Mukan str., 22/5, 050059, Almaty, The Republic of Kazakhstan as the service provider of teamplay.

- There is also a possibility of access to Personal Data during inspection and maintenance of automated procedures or data processing systems.

Вложение 1
Информация о передаче данных

Категории субъектов данных. Передаваемые Персональные данные затрагивают следующие категории субъектов данных:

- сотрудники и поставщики Контролера или группы компаний Контролера;
- пациенты Контролера или группы компаний Контролера.

Виды персональных данных. Передаваемые Персональные данные затрагивают следующие категории данных:

данные о сотруднике, поставщике или данные, связанные с Контролером, такие как контактная информация (например, имя, рабочий адрес, рабочий номер телефона, рабочий адрес электронной почты, рабочий номер мобильного телефона, название должности);

- данные о пациенте, такие как информация, связанная с пациентом (например, атрибуты DICOM, изображения/данные элемента изображения DICOM).

Специальные категории данных. Передаваемые Персональные данные затрагивают следующие специальные категории данных:

- данные о состоянии здоровья, биометрические данные.

Операции по обработке. Передаваемые Персональные данные будут подвергаться следующим основным действиям при Обработке:

тип, предмет Обработки, характер и назначение Обработки Персональных данных указываются в ГСПУ, заключенном между Контролером и ТОО «Сименс Здравоохранение», Республика Казахстан, 050059, г. Алматы, ул. Хаджи Мукана 22/5 в качестве поставщика услуг на платформе teamplay.

- Есть также возможность получить доступ к Персональным данным во время проверки и технического обслуживания автоматических процедур или систем обработки данных.

Attachment TOM

Technical and Organizational Measures (“Attachment TOM”)

1. Pseudonymization and Encryption of Personal Data

Processor separates personal data from the processed data so that it is not possible to link the processed data to an identified or identifiable person without additional information that is stored separately and securely. Processor encrypts personal data with symmetric and asymmetric keys.

2. Confidentiality, Integrity, Availability and Resilience of Systems and Services

a) Processor ensures confidentiality and integrity by taking the following measures:

Access control:

Processor protects its buildings with appropriate access control systems based on a security classification of the buildings and an appropriately defined access authorization concept. All buildings are secured by access control measures using a card reader system. Depending on the security category, property, buildings or individual areas are secured by additional measures. These include special access profiles, biometrics, pin pads, DES dongles, separation locks, video surveillance and security personnel. Access rights for authorized persons are granted individually according to defined criteria. This also applies to external persons.

System access control:

Access to data processing systems is only granted to authenticated users based on a role-based authorization concept using the following measures: Data encryption, individualized password assignment (at least 8 characters, regularly automatic expiration), employee ID cards with PKI encryption, password-protected screen savers in case of inactivity, intrusion detection systems and intrusion-prevention systems, regularly updated antivirus and spyware filters in the network and on the individual PCs and mobile devices.

Data access control:

Приложение TOM

Технические и организационные меры (далее — «Приложение TOM»)

1. Псевдонимизация и шифрование Персональ-ных данных

Обработчик отделяет персональные данные от обработанных данных таким образом, чтобы невозможно было связать обработанные данные с определенным или определяемым лицом без использования дополнительной информации, которая хранится в отдельном и защищенном месте. Обработчик шифрует персональные данные с использованием симметричных и ассиметричных ключей.

2. Конфиденциальность, целостность, доступность и устойчивость систем и услуг

a) Обработчик обеспечивает конфиденциальность и сохранность, принимая следующие меры.

Контроль доступа

Обработчик защищает свои здания соответствующими системами контроля доступа на основании классификации безопасности зданий и установленной должным образом концепции разрешения доступа. Все здания защищены при помощи мер по контролю за доступом с использованием системы считывания карт. В зависимости от категории безопасности собственность, здания и отдельные зоны защищаются при помощи дополнительных мер. К ним относятся специальные профили доступа, биометрические данные, устройства для введения ПИН-кода, электронный DES-ключ, разделительные замки, видеонаблюдение и сотрудники службы безопасности. Права доступа уполномоченным лицам предоставляются индивидуально, в соответствии с установленными критериями. Это также относится к посетителям.

Управление доступом к системе

Доступ к системам обработки данных предоставляется только проверенным пользователям на основании концепции ролевых разрешений с использованием следующих мер: кодировка данных, предоставление индивидуальных паролей (не менее 8 знаков с регулярным автоматическим уведомлением о смене пароля), ID-карты сотрудников с кодировкой PKI, экранная заставка, защищенная паролем на случай отсутствия активности, системы обнаружения вторжения и системы предотвращения вторжения, регулярно обновляемый антивирус и фильтры шпионских программ в сети, на индивидуальных ПК и мобильных устройствах.

Управление доступом к данным

Access to personal data is granted on the basis of a role-based authorization concept. A user management system has been set up, which maps the user database with their respective authorizations and is available centrally in the network for retrieval by requesting data processing systems. Furthermore, data encryption prevents unauthorized access to personal data.

Data transmission control:

Processor secures electronic communication channels by setting up closed networks and data encryption procedures. If a physical data carrier transport takes place, verifiable transport processes are implemented that prevent unauthorized data access or logical loss. Data carriers are disposed of in accordance with data protection regulations.

b) Processor ensures systems and services constant availability and reliability by taking the following measures:

Processor ensures availability and resilience of systems and services by isolating critical IT and network components, by providing adequate backup and redundancy systems, using power redundancy systems, and regularly testing of systems and services. Test and live systems are kept completely separated.

3. Availability and Access to Personal Data in the Event of an Incident

Processor shall restore the availability of and access to personal data in the event of a physical or technical incident by taking the following measures:

Processor stores personal data in RAID systems and integrates redundant systems according to security marking. Processor uses systems for uninterruptible power supplies (e. g. UPS, batteries, generators) to secure the power supply in the data centers.

Databases or data centers are mirrored in different physical locations.

A comprehensive written emergency plan is available. Emergency processes and systems are regularly reviewed.

4. Control Procedures to ensure the Safety of Processing

Processor maintains a control procedure based on a risk-management-based approach, taking into account

Доступ к персональным данным предоставляется на основании концепции ролевых разрешений. Была создана система управления пользователями, которая отображает базу данных пользователей с их соответствующими разрешениями и доступна для централизованного использования в сети для поиска информации путем направления запросов в системы обработки данных. Кроме того, кодировка данных предотвращает несанкционированный доступ к персональным данным.

Управление передачей данных

Обработчик защищает электронные коммуникационные каналы, создавая закрытые сети и процедуры кодировки данных. Если имеет место передача данных на физическом носителе, то используются проверяемые процедуры передачи, которые предотвращают несанкционированный доступ к данным или логические потери. Носители данных уничтожаются в соответствии с требованиями положений по защите данных.

b) Обработчик обеспечивает непрерывный доступ и надежность систем и сервисов, принимая следующие меры.

Обработчик обеспечивает доступность и устойчивость систем и услуг путем изоляции основных ИТ и сетевых компонентов, предоставляя адекватные системы резервного копирования, используя системы бесперебойного питания и регулярного тестирования систем и сервисов. Тестовая и рабочая системы полностью разделены.

3. Наличие и доступ к Персональным данным в случае непредвиденной ситуации

Обработчик обязуется восстановить наличие и доступ к персональным данным в случае физической или технической неполадки, приняв следующие меры.

Обработчик хранит персональные данные в системах RAID и интегрирует резервную систему в соответствии с категорией доступа. Обработчик использует системы с применением источников бесперебойного питания (например, ИБП, аккумуляторы, генераторы) для обеспечения подачи питания в центры данных.

Базы данных или центры данных отображаются в разных местах нахождения.

Разработан в письменном виде всесторонний план действий в чрезвычайной ситуации. Процедуры и системы на случай чрезвычайной ситуации регулярно пересматриваются.

4. Процедуры контроля для обеспечения безопасной обработки

Обработчик поддерживает процедуру контроля на основании подхода с учетом управления рисками,

the basic IT protection catalogues of the Federal Office for Information Security (BSI) and ISO/IEC 27001 requirements for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure security of processing. This ensures the protection of relevant information, applications (including quality and safety test methods), operating environments (e. g. by network monitoring against harmful effects) and the technical implementation of protection concepts (e. g. by means of vulnerability analyses). By systematically detecting and eliminating weak- points, the protective measures are continuously questioned and improved.

5. Personnel Measures

Processor issues written work instructions and regularly trains personnel who have access to personal data to ensure that personal data is only processed in accordance with the law, this DPA and associated instructions of the Customer, including the technical and organizational measures described herein.

принимая во внимание базовые каталоги по защите ИТ Федерального бюро информационной безопасности (BSI) и требования ISO/IEC 27001 относительно регулярной проверки и оценки эффективности технических и организационных мер для обеспечения безопасной обработки. Это обеспечивает защиту необходимой информации, приложений (включая методы проверки качества и безопасности), операционной среды (например, путем мониторинга сети на предмет вредного воздействия) и техническую реализацию концепций защиты (например, путем анализа слабых мест). Путем систематического выявления и устранения слабых мест защитные меры постоянно пересматриваются и совершенствуются.

5. Меры относительно сотрудников

Обработчик разрабатывает письменные рабочие инструкции и регулярно инструктирует сотрудников, которые имеют доступ к персональным данным, чтобы гарантировать, что персональные данные обрабатываются только в соответствии с требованиями законодательства, данного ПОД и соответствующими указаниями Клиента, включая технические и организационные меры, описанные здесь.