PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

СОГЛАШЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ОБЛАЧНЫХ УСЛУГ SAP

1. BACKGROUND

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1 **Purpose and Application.** This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments.

1.1 **Цель и применение.** Условия, содержащиеся в настоящем документе («**Соглашении об обработке персональных данных**»), являются частью Соглашения и соглашением в письменной (в том числе электронной) форме между SAP и Заказчиком. Настоящее Соглашение об обработке персональных данных применяется к отношениям Сторон по обработке данных в связи с предоставлением Облачной услуги в части Персональных данных, обрабатываемых компанией SAP и его Субподрядчиками. Настоящее Соглашение об обработке персональных данных не подлежит применению к отношениям Сторон по поводу непродуктивных сред Облачной услуги, если Заказчику компанией SAP был предоставлен доступ к таким средам, и поэтому Заказчик не должен хранить в них Персональные данные.

1.2 **Structure.** Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

1.2 **Структура.** Приложения 1 и 2 включены в состав настоящего Соглашения об обработке персональных данных и являются его неотъемлемыми частями. В них согласованы предмет, характер и цель обработки, тип Персональных данных, категории субъектов данных и соответствующие технические и организационные меры.

1.3 **GDPR.** SAP and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.3 **GDPR.** SAP и Заказчик соглашаются с тем, что каждая сторона несет ответственность за рассмотрение и принятие требований, предъявляемых к Операторам и Обработчикам Общим регламентом по защите данных 2016/679 («**GDPR**»), в частности в отношении статей 28 и 32-36 указанного регламента, если это применимо (и в той мере, в какой это применимо) к Персональным данным Заказчика или Операторов, которые обрабатываются в соответствии с Соглашением об обработке персональных данных. В качестве иллюстрации в Приложении 3 перечислены соответствующие требования GDPR и разделы настоящего Соглашения об обработке персональных данных.

1.4 **Governance.** SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's

1.4 **Принципы правового регулирования.** В рамках Соглашения об обработке персональных данных SAP выступает в роли Обработчика, а Заказчик и те организации, которым он разрешает использовать Облачную услугу, — в роли Операторов. Заказчик выступает в качестве единственного контактного лица и несет единоличную ответственность за получение любых соответствующих полномочий, одобрений и разрешений для обработки Персональных данных в соответствии с настоящим Соглашением об обработке персональных данных, включая, в соответствующих ситуациях, подтверждение Операторами привлечения SAP в качестве Обработчика. Если Заказчик предоставляет полномочия, одобрения, поручения или разрешения, они предоставляются не только от

responsibility to forward such information and notices to the relevant Controllers.

имени самого Заказчика, но и от имени всех остальных Операторов, использующих Облачную услугу. В тех случаях, когда SAP информирует или уведомляет Заказчика, такая информация или уведомление считается полученной теми Операторами, которым Заказчик разрешил использовать Облачную услугу, и Заказчик несет ответственность за передачу такой информации и уведомлений соответствующим Операторам.

2. SECURITY OF PROCESSING

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

2. БЕЗОПАСНОСТЬ ОБРАБОТКИ

2.1 Соответствующие технические и организационные меры. Компания SAP внедрила и будет применять технические и организационные меры, определенные в Приложении 2. Заказчик изучил эти меры и согласен с приемлемостью мер в отношении Облачной услуги, выбранной им в Договоре, с учетом текущего уровня развития науки и техники, затрат на реализацию, характера, сферы применения, контекста и целей обработки Персональных данных.

2.2 Изменения. SAP применяет определенные в Приложении 2 технические и организационные меры ко всем заказчикам SAP, обслуживаемым в одном Центре обработки данных и получающим одну и ту же Облачную услугу. SAP может в любое время без предварительного уведомления изменить меры, определенные в Приложении 2, если при этом сохранится сопоставимый или более высокий уровень безопасности. Индивидуальные мероприятия могут быть заменены новыми мерами, если они служат той же цели и не уменьшают уровень безопасности Персональных данных.

3. SAP OBLIGATIONS

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

3.2 Processing on Legal Requirement. SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform

3. ОБЯЗАТЕЛЬСТВА КОМПАНИИ SAP

3.1 Поручения Заказчика. SAP обязано обрабатывать Персональные данные только в соответствии с документально подтвержденными поручениями Заказчика. К такому документально подтвержденному первоначальному поручению относится Соглашение (в том числе и настоящее Соглашение об обработке персональных данных), а дополнительные поручения формируются при каждом случае использования Облачной услуги. SAP обязуется прилагать разумные усилия для выполнения любых других поручений Заказчика, если того требует Законодательство о защите персональных данных и это технически осуществимо и не требует изменений в Облачной услуге. Если применимо какое-либо из вышеупомянутых исключений или SAP не может выполнить поручение по иным причинам либо придерживается мнения, что поручение нарушает Законодательство о защите персональных данных, SAP незамедлительно уведомляет об этом Заказчика (допускается уведомление по электронной почте).

3.2 Обработка, основанная на требовании законодательства. SAP также может обрабатывать Персональные данные, если того

Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

требует применимое законодательство. В этом случае компания SAP должна уведомить Заказчика о таком требовании законодательства перед обработкой, если такое информирование не запрещено законодательством по уважительным причинам в государственных интересах.

3.3 Personnel. To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

3.3 Персонал. В связи с обработкой Персональных данных компания SAP и ее Субподрядчики по обработке данных должны предоставлять доступ только уполномоченному персоналу, который обязался обеспечить конфиденциальность. Компания SAP и ее Субподрядчики по обработке данных проводят среди персонала, имеющего доступ к Персональным данным, регулярные инструктажи по надлежащим мерам защиты данных и конфиденциальности.

3.4 Cooperation. At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.4 Сотрудничество. По запросу Заказчика SAP окажет Заказчику или любому Оператору содействие в обработке запросов со стороны Субъектов данных и контролирующих органов, относящихся к обработке SAP Персональных данных или любого нарушения их конфиденциальности. SAP обязуется как можно скорее уведомлять Заказчика о любом запросе, полученном им от Субъекта данных в связи с обработкой Персональных данных, не отвечая на этот запрос без дальнейших поручений Заказчика, если это применимо. SAP предоставит функциональные возможности, которые позволят Заказчику исправлять или удалять Персональные данные из Облачной услуги или ограничивать их обработку в соответствии с Законодательством о защите персональных данных. Если такая функциональность не предоставляется, SAP будет исправлять или удалять любые Персональные данные или ограничивать ее обработку в соответствии с поручением Заказчика и Законодательством о защите персональных данных.

3.5 Personal Data Breach Notification. SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.

3.5 Уведомление о Нарушении конфиденциальности персональных данных. SAP обязуется без каких-либо необоснованных задержек уведомлять Заказчика о ставших известными фактах Нарушения конфиденциальности персональных данных и предоставить в разумных пределах имеющуюся информацию о таких фактах, чтобы помочь Заказчику выполнить его обязательства в отношении информирования о Нарушении конфиденциальности персональных данных в соответствии с требованиями Законодательства о защите персональных данных. SAP может предоставлять такую информацию поэтапно, по мере того, как она становится доступной. Такое уведомление не должно интерпретироваться или толковаться как признание ошибки или ответственности со стороны SAP.

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers)

3.6 Оценка воздействия на персональные данные. Если в соответствии с Законодательством

are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

о защите персональных данных Заказчик (или его Операторы) должны выполнить оценку воздействия на персональные данные или провести предварительную консультацию с контролирующим органом, SAP по запросу Заказчика предоставит соответствующие документы, которые обычно оформляются при оказании Облачной услуги (например, настоящее Соглашение об обработке персональных данных, Соглашение, отчеты о проверках или сертификаты). Любая дополнительная помощь должна быть взаимно согласована между Сторонами.

4. DATA EXPORT AND DELETION

4. ЭКСПОРТ И УДАЛЕНИЕ ДАННЫХ

4.1 **Export and Retrieval by Customer.** During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Personal Data.

4.1 **Экспорт и извлечение данных Заказчиком.** В течение Срока подписки Заказчик в любое время имеет доступ к своим Персональным данным в соответствии с условиями Соглашения. Заказчик имеет право экспортировать и извлекать свои Персональные данные в стандартном формате. Если на операции экспорта и извлечения распространяются технические ограничения, SAP и Заказчик обязуются определить обоснованный способ, обеспечивающий доступ Заказчика к своим Персональным данным.

4.2 **Deletion.** Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

4.2 **Удаление.** До истечения Срока подписки Заказчик может использовать доступные инструменты SAP для самостоятельного экспорта, чтобы окончательно экспортировать Персональные данные из Облачной услуги (что должно толковаться как «возврат» Персональных данных). По истечении Срока подписки Заказчик настоящим поручает SAP удалить Персональные данные, оставшиеся на серверах, где размещена Облачная услуга, в течение обоснованного периода времени в соответствии с Законодательством о защите персональных данных (не более шести месяцев), если применимое законодательство не требует дальнейшего их хранения.

5. CERTIFICATIONS AND AUDITS

5. СЕРТИФИКАТЫ И АУДИТ

5.1 **Customer Audit.** Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

5.1 **Аудит, проводимый Заказчиком.** Заказчик или его независимый внешний аудитор, приемлемый в разумных пределах для SAP (привлечение внешних аудиторов, которые являются конкурентами SAP, не имеют соответствующей квалификации или не являются независимыми, недопустимо), могут проверить средства осуществления контроля SAP и методы обеспечения безопасности, применяемые SAP при обработке Персональных данных, только в следующих случаях:

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's

(a) Компания SAP не представила достаточных свидетельств соблюдения технических и организационных мер, защищающих продуктивные системы Облачной услуги, одним из следующих способов: (i) предоставив сертификат соответствия стандарту ISO 27001 или иным стандартам (в объеме, указанном в сертификате); (ii) предоставив действительный аттестационный

request audit reports or ISO certifications are available through the third party auditor or SAP;

отчет ISAE3402 и (или) ISAE3000 либо другой отчет SOC1-3. По запросу Заказчика аудиторские отчеты или сертификацию на соответствие стандартам ISO выполняет либо внешний аудитор, либо SAP.

(b) A Personal Data Breach has occurred;

(b) Произошло Нарушение конфиденциальности персональных данных.

(c) An audit is formally requested by Customer's data protection authority; or

(c) Получен формальный запрос на проверку от уполномоченного органа по защите данных Заказчика.

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

(d) Императивными нормами Законодательства о защите персональных данных прямо предусмотрено право Заказчика на проверку (аудит) при условии, что Заказчик будет проводить такую проверку один раз в любой двенадцатимесячный период, если только Законодательством о защите данных не предусмотрены более частые проверки.

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.2 Аудит, проводимый другим Оператором. Любой другой Оператор может проверять средства осуществления контроля SAP и методы обеспечения безопасности, относящиеся к обрабатываемым SAP Персональным данным, в соответствии с разделом 5.1, только если к нему применимы основания, перечисленные в разделе 5.1. Такая проверка должна проводиться через Заказчика в соответствии с разделом 5.1, кроме случаев, когда такой другой Оператор должен осуществлять ее самостоятельно в соответствии с Законодательством о защите персональных данных. Если проведения проверки требуют сразу несколько Операторов, чьи Персональные данные обрабатываются SAP на основе Соглашения, Заказчик должен принять все разумные меры для объединения таких проверок во избежание многократного проведения аудита.

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

5.3 Объем аудита. Заказчик обязан заблаговременно уведомлять SAP о любом аудите не позднее чем за шестьдесят дней до его проведения, кроме случаев, когда императивными нормами Законодательства о защите данных или требованием компетентного органа по защите данных предусмотрен более короткий период для уведомления. Частота и объем любых проверок должны быть взаимно согласованы между сторонами и проводиться обоснованно и добросовестно. Проведение проверок Заказчиком должно быть ограничено тремя рабочими днями. Помимо этих ограничений стороны обязуются использовать действующие сертификаты или отчеты других аудиторов или проверяющих организаций, чтобы избежать повторные проверки или свести их к минимуму. Заказчик обязан представлять SAP результаты всех проверок.

5.4 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has

5.4 Затраты на проведение аудита. Заказчик несет расходы по любой проверке, если в ходе ее проведения не будут выявлены существенные нарушения настоящего Соглашения об обработке персональных данных со стороны SAP, в случае

breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

чего расходы по аудиту будет нести SAP. Если аудиторская проверка выявит, что SAP нарушает свои обязательства по Соглашению об обработке персональных данных, SAP немедленно устранит нарушение за собственный счет.

6. SUBPROCESSORS

6. СУБПОДРЯДЧИКИ ПО ОБРАБОТКЕ ДАННЫХ

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

6.1 Разрешенное использование. SAP имеет право и соответствующее разрешение на передачу обработки Персональных данных Субподрядчикам по обработке данных при условии, что:

(a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

(a) SAP или SAP SE будут от своего имени привлекать Субподрядчиков по обработке данных на основании договора, заключаемого в письменной (в том числе в электронной) форме в соответствии с условиями настоящего Соглашения об обработке персональных данных в той части, которая касается выполнения такой обработки Субподрядчиком по обработке данных. SAP несет ответственность за любые нарушения Субподрядчика по обработке данных в соответствии с условиями настоящего Соглашения.

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

(b) Перед выбором Субподрядчика по обработке данных SAP будет оценивать применяемые им методы обеспечения безопасности, неприкосновенности и конфиденциальности данных, чтобы установить, способен ли он обеспечить уровень защиты Персональных данных, требуемый в рамках настоящего Соглашения об обработке персональных данных.

(c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.

(c) Актуальный список Субподрядчиков SAP по обработке данных на момент вступления в силу Соглашения публикуется SAP или предоставляется Заказчику по запросу. Для каждого Субподрядчика по обработке данных, привлекаемого SAP для предоставления Облачной услуги, указывается имя, адрес и роль.

6.2 New Subprocessors. SAP's use of Subprocessors is at its discretion, provided that:

6.2 Новые Субподрядчики по обработке данных. SAP пользуется услугами Субподрядчиков по обработке данных на свое усмотрение при соблюдении следующих условий:

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

(a) SAP будет заранее информировать Заказчика (по электронной почте или путем публикации на портале поддержки, доступ к которому предоставляет служба сопровождения SAP) о любом предполагаемом добавлении нового или замене текущего Субподрядчика по обработке данных с указанием имен, адресов и ролей.

(b) Customer may object to such changes as set out in Section 6.3.

(b) Заказчик может возражать против таких изменений в соответствии с разделом 6.3.

6.3 Objections to New Subprocessors.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

(b) Within the thirty day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the thirty day period.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

6.3 Возражения против новых Субподрядчиков по обработке данных.

(a) Если в соответствии с Законодательством о защите персональных данных у Заказчика есть законная причина возражать против обработки Персональных данных новыми Субподрядчиками по обработке данных, Заказчик может расторгнуть Соглашение (в том, что касается Облачной услуги, для которой будет привлекаться новый Субподрядчик по обработке данных), уведомив об этом SAP в письменной форме. Такое расторжение вступает в силу в момент, установленный Заказчиком, но не позднее тридцати дней со дня получения им уведомления от SAP о новом Субподрядчике по обработке данных. Если в течение тридцати дней после получения уведомления Заказчик не расторг Соглашение, считается, что он согласен с привлечением нового Субподрядчика по обработке данных.

(b) В течение тридцатидневного периода со дня уведомления Заказчика компанией SAP о новом Субподрядчике по обработке данных Заказчик может потребовать, чтобы стороны добросовестно обсудили разрешение противоречий. Такие обсуждения не продлевают период для расторжения и не влияют на право SAP привлекать новых Субподрядчиков по обработке данных после тридцатидневного периода.

(c) При этом считается, что расторжение в соответствии с настоящим разделом 6.3 происходит не по вине одной из сторон и осуществляется в соответствии с условиями Соглашения.

6.4 Экстренная замена. SAP может заменить Субподрядчика по обработке данных без предварительного уведомления, если причина такой замены находится вне контроля SAP и она требуется незамедлительно для обеспечения безопасности или в связи с другими неотложными потребностями. В этом случае SAP уведомляет Заказчика о замене Субподрядчика по обработке данных сразу же, как только это становится возможным после его назначения. При этом соответственно применяется раздел 6.3.

7. МЕЖДУНАРОДНАЯ ОБРАБОТКА ДАННЫХ

7.1 Условия международной обработки данных. SAP имеет право обрабатывать Персональные данные, в том числе с привлечением Субподрядчиков по обработке данных, в соответствии с настоящим Соглашением об обработке персональных данных за пределами страны места нахождения Заказчика, согласно нормам Законодательства о защите персональных данных.

7.2 **Standard Contractual Clauses.** Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

(a) SAP and Customer enter into the Standard Contractual Clauses;

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

7.3 **Relation of the Standard Contractual Clauses to the Agreement.** Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.2 **Стандартные договорные условия.** В случае, если (i) Персональные данные Оператора из ЕЭЗ или Швейцарии обрабатываются в стране за пределами ЕЭЗ, Швейцарии и любых стран, организаций или территорий, признанных Европейским Союзом в качестве безопасной страны с адекватным уровнем защиты данных согласно ст. 45 GDPR, а также если (ii) Персональные данные другого Оператора обрабатываются трансгранично и для такой трансграничной обработки требуются средства обеспечения адекватности в соответствии с законодательством страны Оператора, и такие требуемые средства можно обеспечить путем заключения Стандартных договорных условий, применяются следующие положения:

(a) SAP и Заказчик заключают Стандартные договорные условия.

(b) Заказчик заключает Стандартные договорные условия с каждым соответствующим Субподрядчиком по обработке данных следующим образом: (i) присоединяется к Стандартным договорным условиям, заключенным между SAP или SAP SE и Субподрядчиком по обработке данных, в качестве независимого обладателя прав и обязательств («Модель присоединения») или (ii) самостоятельно заключает Стандартные договорные условия с представленным SAP Субподрядчиком по обработке данных («Модель доверенности»). Модель доверенности применяется, если и когда SAP прямо подтвердит, что Субподрядчик по обработке данных имеет право на ее использование, добавив его в список Субподрядчиков по обработке данных, указанный в разделе 6.1(c), или уведомив об этом Заказчика.

(c) Другие Операторы, которым Заказчик разрешил использовать Облачные услуги в соответствии с Соглашением, могут также заключать с SAP и (или) соответствующими Субподрядчиками по обработке данных Стандартные договорные условия таким же образом, как Заказчик, в соответствии с положениями, изложенными выше в разделах 7.2 (a) и (b). В этом случае Заказчик будет заключать Стандартные договорные условия от имени других Операторов.

7.3 **Связь между Соглашением и Стандартными договорными условиями.** Никакие положения Соглашения не имеют преимущественную силу над какими-либо противоречащими им положениями Стандартных договорных условий. Во избежание недоразумений следует уточнить, что дополнительные определения правил аудита и привлечения субподрядчиков, изложенные в разделах 5 и 6 настоящего Соглашения об обработке персональных данных, применяются

также в отношении Стандартных договорных условий.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

7.4 Применимое законодательство в Стандартных договорных условиях. Стандартные договорные условия регулируются законодательством страны, в которой зарегистрирован соответствующий Оператор.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

8. ДОКУМЕНТАЦИЯ И ВЕДЕНИЕ УЧЕТА ОБРАБОТКИ

Каждая сторона несет ответственность за соблюдение ею требований к документации, в частности ведению учета обработки в случаях, когда это требуется в соответствии с Законодательством о защите персональных данных. Каждая сторона должна в пределах разумного помогать другой стороне в соблюдении требований к документации, в том числе предоставляя необходимую другой стороне информацию тем способом, который обоснованно запрашивает такая другая сторона (например, с использованием электронной системы), с тем чтобы последняя смогла выполнить все свои обязательства, связанные с ведением учета обработки.

9. EU ACCESS

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. SAP shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply.

9.2 EU Access. SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4.

9.3 Data Center Location. Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a Data Center within the EEA or to Switzerland, SAP will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

9. ДОСТУП ЕС

9.1 Дополнительные услуги. Доступ ЕС — это дополнительная услуга, которую может предложить SAP. SAP предоставляет такую Облачную услугу, для которой предоставлен Доступ ЕС, исключительно для продуктивных инсталляций в соответствии с настоящим разделом 9. Если Доступ ЕС в Договоре явным образом не указан и не согласован, настоящий раздел 9 не применяется.

9.2 Доступ ЕС. Для обеспечения услуг по сопровождению, требующих доступа к Персональным данным в Облачной услуге, SAP будет привлекать только Европейских субподрядчиков по обработке данных. SAP не будет экспортировать Персональные данные за пределы ЕЭЗ или Швейцарии, кроме случаев, когда это явно не разрешено Заказчиком в письменной форме в каждом конкретном случае (разрешение может быть предоставлено по электронной почте) или является исключением, предусмотренным разделом 9.4.

9.3 Место нахождения Центра обработки данных. Начиная с даты вступления Соглашения в силу, Центры обработки данных, используемые для размещения Персональных данных в Облачной услуге, располагаются в ЕЭЗ или Швейцарии. SAP обязуется не переносить инсталляцию Заказчика в Центр обработки данных за пределами ЕЭЗ и Швейцарии без предварительного письменного согласия Заказчика (которое может быть предоставлено по электронной почте). Если SAP планирует перенести инсталляцию Заказчика в Центр обработки данных за пределами ЕЭЗ и Швейцарии, SAP уведомит об этом Заказчика в письменной форме не позднее чем за тридцать дней до планируемого перевода.

9.4 Exclusions. The following Personal Data is not subject to 9.2 and 9.3:

(a) Contact details of the sender of a support ticket; and

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP.

9.4 Исключения. Требования разделов 9.2 и 9.3 не распространяются на следующие Персональные данные:

(a) Контактные данные отправителя запросов на сопровождение.

(b) Любые другие Персональные данные, предоставленные Заказчиком при оформлении запроса на сопровождение. Заказчик имеет право отказаться от передачи Персональных данных при оформлении запроса на сопровождение. Если такие данные необходимы в ходе разрешения инцидента, Заказчик может выполнить обезличивание всех Персональных данных перед передачей сообщения об инциденте в SAP.

10. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

10.1 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

10.2 "Data Center" means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form.

10.3 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

10. ОПРЕДЕЛЕНИЯ

Все термины, написанные с заглавной буквы и не определенные в настоящем документе, употребляются в значениях, установленных в Соглашении.

10.1 «Оператор» означает физическое или юридическое лицо, государственный орган, учреждение или другую организацию, которые самостоятельно или совместно с другими лицами определяют цели и способы обработки Персональных данных. Для целей настоящего Соглашения об обработке персональных данных в случае, когда Заказчик выступает в качестве Обработчика для другого Оператора, в контексте взаимодействия с SAP он должен рассматриваться в качестве дополнительного и независимого Оператора с соответствующими правами и обязательствами по настоящему Соглашению об обработке персональных данных.

10.2 «Центр обработки данных» означает место размещения продуктивного экземпляра (инсталляции) Облачной услуги для Заказчика в соответствующем регионе, которое указано на сайте: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html или в уведомлении, направленном Заказчику, или иным образом согласовано сторонами в Договоре.

10.3 «Законодательство о защите персональных данных» означает применимое законодательство, защищающее базовые права и свободы людей и право на неприкосновенность частной жизни в связи с обработкой Персональных данных по Соглашению (и в том, что касается отношений между сторонами в связи с обработкой Персональных данных компанией SAP по поручению Заказчика, включает GDPR в качестве минимального стандарта, независимо от того, распространяется ли действие GDPR на Персональные данные).

10.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

10.4 **«Субъект данных»** означает определенное или определяемое физическое лицо, как этот термин установлен в Законодательстве о защите персональных данных.

10.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

10.5 **«ЕЭЗ»** означает Европейскую экономическую зону, а именно: государства-члены Европейского Союза, а также Исландию, Лихтенштейн, Норвегию.

10.6 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

10.6 **«Европейский субподрядчик по обработке»** означает Субподрядчика по обработке, который физически осуществляет обработку Персональных данных на территории ЕЭЗ или Швейцарии.

10.7 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

10.7 **«Персональные данные»** означают любую информацию, относящуюся к Субъекту данных и охраняемую Законодательством о защите персональных данных. Для целей Соглашения об обработке персональных данных к ним относятся только Персональные данные, которые (i) введены Заказчиком или его Авторизованными пользователями в среду Облачной услуги или получена ими в связи с ее использованием; (ii) предоставлены компании SAP или ее Субподрядчиками по обработке данных либо используются ими с целью оказания услуг по сопровождению по Соглашению. Персональные данные — это подмножество Данных заказчика (как этот термин определен в Соглашении).

10.8 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

10.8 **«Нарушение конфиденциальности персональных данных»** означает подтвержденное (1) случайное или незаконное уничтожение, утрату, изменение, несанкционированное раскрытие Персональных данных или несанкционированный доступ к ним третьих лиц; (2) аналогичный инцидент, связанный с Персональными данными, в случае которого Оператор в соответствии с Законодательством о защите персональных данных должен уведомлять компетентные органы по защите данных или Субъекты данных.

10.9 **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

10.9 **«Обработчик»** означает физическое или юридическое лицо, государственный орган, учреждение или другую организацию, которые обрабатывают персональные данные по поручению оператора, будь то непосредственно в качестве его обработчика или косвенно в качестве субподрядчика обработчика, который обрабатывает Персональные данные от имени оператора.

10.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereof as Appendix 4.

10.10 **«Стандартные договорные условия»**, также называемые «Типовые условия ЕС», означает условия, описанные в приложении «Стандартные договорные условия (обработчики)», и любых последующих версиях этого документа, опубликованных Европейской комиссией (и применяемых автоматически). Стандартные договорные условия в редакции на дату вступления в силу Соглашения приведены в качестве Приложения 4.

10.11 "Subprocessor" means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

10.11 «Субподрядчик по обработке данных» означает Аффилированных лиц SAP, SAP SE, Аффилированных лиц SAP SE и третьих лиц, привлекаемых SAP, SAP SE или Аффилированными лицами SAP SE в связи с предоставлением Облачной услуги и обрабатывающих Персональные данные в рамках настоящего Соглашения об обработке персональных данных.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer

SAP and its Subprocessors provide the Cloud Service that includes the following support:

SAP SE Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

SAP SE Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Приложение 1 к Соглашению об обработке персональных данных и, если применимо, Стандартным договорным условиям

Экспортер данных

Экспортер данных — это Заказчик, который подписался на Облачную услугу, позволяющую Авторизованным пользователям вводить, изменять, использовать, удалять или иным образом обрабатывать Персональные данные. В тех случаях, когда Заказчик позволяет другим Операторам также использовать Облачную услугу, эти другие Операторы также являются Экспортерами данных.

Импортер данных

Компания SAP и ее Субподрядчики по обработке предоставляют Облачную услугу, которая включает следующие услуги по сопровождению:

Аффилированные лица SAP SE оказывают услуги по сопровождению для Центров обработки данных, где размещается Облачная услуга, удаленно с объектов SAP, находящихся в Санкт-Леон-Роте (Германия), Индии и других местах, где компания SAP нанимает персонал для операционной деятельности или оказания Облачных услуг. К сопровождению относятся:

- мониторинг Облачной услуги;
- резервное копирование и восстановление Данных заказчика, хранимых в рамках оказания Облачной услуги;
- разработка и выпуск исправлений и обновлений для Облачной услуги;
- мониторинг, поиск неисправностей и управление основной инфраструктурой и базой данных Облачной услуги;
- мониторинг безопасности, сопровождение систем обнаружения сетевых атак, проведение тестов на проникновение.

Аффилированные лица SAP SE оказывают услуги по сопровождению в тех случаях, когда Заказчик подает запрос на сопровождение на такие услуги в связи с недоступностью Облачной услуги для всех или части Авторизованных пользователей или отклонениями в ее работе. SAP отвечает на телефонные звонки и выполняет базовый поиск неисправностей, направляет и обрабатывает запросы на сопровождение в системе отслеживания, отделенной от продуктивной инсталляции Облачной услуги.

Субъекты данных

Кроме случаев, когда Экспортером данных установлено иное, переданные Персональные данные относятся к следующим категориям Субъектов данных: сотрудники, работники по гражданско-правовым соглашениям, деловые партнеры и прочие лица, Персональные данные которых хранятся в Облачной услуге.

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

Категории данных

Передаваемые Персональные данные касаются следующих категорий данных:

Заказчик определяет категории данных по каждой Облачной услуге, на которую он подписался. Заказчик может настроить поля данных при внедрении Облачной услуги или иным образом, предусмотренным Облачной услугой. Передаваемые Персональные данные обычно включают следующие категории данных: имя, номер телефона, адрес электронной почты, часовой пояс нахождения субъекта, адрес, данные для доступа к системе, авторизации и использования системы, название компании, данные о контрактах и счетах, а также данные конкретных приложений, вводимые Авторизованными пользователями в рамках пользования Облачной услугой, в том числе сведения о банковском счете, кредитных и дебетовых картах.

Особые категории данных (если применимо)

Передаваемые Персональные данные касаются следующих особых категорий данных: согласно указанному в Соглашении (в том числе Договоре), если это применимо.

Операции и цели обработки

Обработка передаваемых Персональных данных предполагает следующие основные операции и цели:

- использование Персональных данных для настройки, управления и наблюдения за Облачной услугой (включая Услуги по операционному и техническому сопровождению);
- предоставление Консультационных услуг;
- передача информации Авторизованным пользователям;
- хранение Персональных данных в выделенных Центрах обработки данных (многопользовательская архитектура);
- загрузка в Облачную услугу исправлений и обновлений;
- резервное копирование Персональных данных;
- компьютерная обработка Персональных данных, включая передачу, извлечение данных и доступ к ним;
- сетевой доступ в целях разрешения передачи Персональных данных;
- исполнение поручений Заказчика согласно Соглашению.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.

- **TOMs Set 2**: applies to the TOMs Set 2 Services only. As of July 1, 2020, "**TOMs Set 2 Services**" means the following Cloud Services: SAP Analytics Cloud. SAP may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1.

TOMs SET 1

Last Updated: April 2018

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.

Приложение 2 к Соглашению об обработке персональных данных и, если применимо, Стандартным договорным условиям — технические и организационные меры

Настоящее Приложение 2 содержит две группы технических и организационных мер ("**ТОМ**"):

- **Группа ТОМ 1 (последнее обновление в Апреле 2018, без изменений):** применяется ко всем Облачным услугам, за исключением услуг, к которым применима Группа ТОМ 2.

- **Группа ТОМ 2**: применяется только к Услугам Группы ТОМ 2. На 1 июля 2020, "**Услуги Группы ТОМ 2**" включают следующие Облачные услуги: SAP Analytics Cloud. Время от времени SAP вправе исключать Облачные услуги из перечня Услуг Группы ТОМ 2. В этом случае к таким Облачным услугам будут применяться Группа ТОМ 1.

Группа ТОМ 1

Последнее обновление: Апрель 2018

1. ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕРЫ

В следующих разделах определяются текущие технические и организационные меры SAP. SAP может менять эти меры в любой момент без уведомления при условии обеспечения аналогичного или более высокого уровня безопасности. Индивидуальные мероприятия могут быть заменены новыми мерами, если они служат той же цели и не уменьшают уровень безопасности Персональных данных.

1.1 Контроль физического доступа. Необходимо предотвратить физический доступ несанкционированных лиц на объекты, в здания и помещения, где размещаются системы обработки данных, используемые для обработки Персональных данных и/или их использования.

Меры:

- SAP защищает свое имущество и объекты, используя соответствующие средства в соответствии с Политикой безопасности SAP
- В целом здания защищены посредством систем контроля доступа (например, системы доступа по смарт-картам).
- Минимальным требованием является оснащение внешних входов в здания сертифицированной системой ключей, обеспечивающей современное активное управление ключами.
- Могут быть реализованы дополнительные меры обеспечения безопасности зданий, отдельных территорий и прилегающих объектов с учетом классификации безопасности. Сюда относятся конкретные профили доступа, видеонаблюдение, системы тревожной сигнализации и системы биометрического контроля доступа.

- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.

- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy

- All personnel access SAP's systems with a unique identifier (user ID).

- SAP has procedures in place to so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.

- Права доступа предоставляются уполномоченным лицам на индивидуальной основе в соответствии с мерами по контролю системы и доступа к данным (см. пункты 1.2 и 1.3 ниже). Эти меры также распространяются на доступ посетителей. Гости и посетители зданий SAP обязаны зарегистрироваться на входе, сообщив свое имя, и далее следовать в сопровождении уполномоченных сотрудников компании.

- Работники SAP и сторонний персонал должны иметь при себе идентификационные карты на всех объектах SAP.

Дополнительные меры для Центров обработки данных:

- Во всех Центрах обработки данных необходимо следовать строгим процедурам безопасности с привлечением специалистов по охране и использованием камер наблюдения, детекторов движения, устройств контроля доступа и других средств, позволяющих устранить угрозы безопасности для оборудования и помещений Центра обработки данных. Только уполномоченные представители имеют доступ к системам и инфраструктуре в помещениях Центров обработки данных. В целях поддержания правильного функционирования оборудования обеспечения физической безопасности (датчиков движения, камер и т. д.) проводится регулярное обслуживание оборудования.

- SAP и все сторонние провайдеры Центров обработки данных фиксируют имена и время прибытия уполномоченного персонала на закрытые территории в составе Центров обработки данных.

1.2 Контроль доступа к системам. Несанкционированный доступ к системам обработки данных, используемым для предоставления Облачной услуги, должен быть закрыт.

Меры:

- Доступ к уязвимым системам, в том числе используемым для хранения и обработки Персональных данных, предоставляется по модели многоуровневой авторизации. Управление разрешениями осуществляется посредством определенных процессов в соответствии с Политикой безопасности SAP.

- Весь персонал входит в системы SAP только на основании уникального идентификатора (идентификатора пользователя).

- В SAP действуют процессы, обеспечивающие внедрение запрашиваемых изменений полномочий строго в соответствии с Политикой безопасности SAP (например, никакие права не предоставляются без соответствующего разрешения). Если сотрудник покидает компанию, его права доступа аннулируются.

- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- В SAP действует политика паролей, запрещающая совместное использование и обмен паролями, предписывающая порядок действий в случае раскрытия пароля и устанавливающая требования о регулярной смене паролей и изменении паролей по умолчанию. Для аутентификации назначаются персональные идентификаторы пользователей. Все пароли должны соответствовать минимальным установленным требованиям и храниться в зашифрованной форме. В системе реализована принудительная смена доменных паролей каждые шесть месяцев и действуют определенные требования к сложности паролей. На каждом компьютере имеется защищенная паролем экранная заставка.

- The company network is protected from the public network by firewalls.

- Сеть компании защищена от общедоступной сети брандмауэром.

- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

- SAP использует современные антивирусные программы на точках доступа в сеть компании (для учетных записей электронной почты), а также на всех файловых серверах и всех рабочих станциях.

- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

- Для гарантированного регулярного развертывания необходимых обновлений безопасности используется программа управления программными вставками для системы безопасности. Полный удаленный доступ к корпоративной сети и критически важной инфраструктуре SAP защищен с помощью строгой аутентификации.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

1.3 Контроль доступа к данным Лица, уполномоченные использовать системы обработки данных, должны иметь доступ только к тем Персональным данным, в отношении которых у них есть право доступа; просмотр, копирование, изменение или удаление Персональных данных в ходе обработки, использования и хранения без соответствующего разрешения запрещено.

Measures:

Меры:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

- В соответствии с Политикой безопасности SAP необходимо обеспечить защиту Персональных данных по меньшей мере на уровне защиты конфиденциальных данных в соответствии со стандартом SAP по классификации информации.

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.

- Доступ к Персональным данным предоставляется только по служебной необходимости. Персонал имеет доступ к информации, необходимой ему для выполнения своих обязанностей. В SAP используются концепции полномочий, в рамках которых для каждой учетной записи (идентификатора пользователя) документируются процессы предоставления и назначения ролей. Все Данные заказчика защищены в соответствии с Политикой безопасности SAP.

- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal

- Все производственные серверы работают в соответствующих Центрах обработки данных или серверных помещениях. Меры безопасности, которые защищают приложения, используемые для обработки Персональных данных, регулярно

and external security checks and penetration tests on its IT systems.

- SAP does not allow the installation of software that has not been approved by SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

Measures:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.

проверяются. Для этого SAP проводит внутренние и внешние проверки безопасности и тесты на проникновение в свои ИТ-системы.

- SAP не разрешает установку программного обеспечения, не утвержденного SAP.
- Методы уничтожения данных и носителей данных, после того как они больше не требуются, определяются правилами безопасности SAP.

1.4 Контроль передачи данных. За исключением случаев, когда это необходимо для оказания Облачных услуг в соответствии с Соглашением, запрещается без разрешения просматривать, копировать, изменять или удалять Персональные данные во время передачи. В случае физической транспортировки носителей данных компания SAP обязана принять адекватные меры для обеспечения согласованных уровней обслуживания (например, шифрование и освинцованные контейнеры).

Меры:

- При передаче по внутренним сетям SAP Персональные данные защищаются в соответствии с Политикой безопасности SAP.
- Если данные передаются между компанией SAP и Заказчиком, меры по защите передаваемых Персональных данных согласуются сторонами и включаются в соответствующее соглашение. Это условие применяется к физическому переносу данных и переносу данных по сети. В любом случае Заказчик берет на себя ответственность за любое перемещение данных за пределами подконтрольных SAP систем (например, при переносе данных за пределы брандмауэра Центра обработки данных SAP).

1.5 Контроль ввода данных. Необходимо обеспечить возможность ретроспективного изучения и установления факта ввода, изменения или удаления Персональных данных в системах обработки данных SAP.

Меры:

- Компания SAP разрешает доступ к Персональным данным только авторизованному персоналу, в необходимом для работы объеме.
- Компания SAP внедрила систему регистрации ввода, изменения, удаления и блокировки Персональных данных сотрудниками SAP или ее Субподрядчиками по обработке данных в той степени, в которой это возможно в рамках предоставления Облачной услуги.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

- SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.

1.6 Контроль заданий. Обрабатываемые по заказу Персональные данные (например, Персональные данные, обрабатываемые по запросу заказчика) следует обрабатывать исключительно согласно условиям Соглашения и сопутствующих указаний Заказчика.

Меры:

- Компания SAP использует средства контроля и процессы, позволяющие следить за выполнением положений договоров между SAP и ее заказчиками, субподрядчиками по обработке данных и другими поставщиками услуг.
- В соответствии с Политикой безопасности SAP необходимо обеспечить защиту Персональных данных по меньшей мере на уровне защиты конфиденциальных данных в соответствии со стандартом SAP по классификации информации.
- Все работники, субподрядчики по обработке данных и прочие поставщики услуг SAP связаны договорными обязательствами соблюдать конфиденциальность всей уязвимой информации, включая промышленные секреты заказчиков и партнеров SAP.

1.7 Контроль доступности. Необходимо защищать Персональные данные от случайного или несанкционированного уничтожения или потери.

Меры:

- SAP использует процессы регулярного резервного копирования для обеспечения возможности восстановления критически важных бизнес-систем по мере необходимости.
- SAP использует источники бесперебойного питания (например, ИБП, аккумуляторы, генераторы и т. д.), чтобы поддержать непрерывную работу систем электропитания Центров обработки данных.
- Компания SAP определила планы для внештатных ситуаций в связи с критически важными для бизнеса процессами и может предложить стратегии аварийного восстановления критически важных для бизнеса служб, подробно описанные в Документации или включенные в Договор для соответствующей Облачной услуги.
- Регулярно проводятся испытания аварийных процессов и систем.

1.8 Контроль разделения данных. Персональные данные, собранные в разных целях, могут обрабатываться по отдельности.

Меры:

- SAP использует технические возможности развернутого программного обеспечения (например, многопользовательские или раздельные системные ландшафты) для разделения Персональных данных от разных заказчиков.

- Customer (including its Controllers) has access only to its own data.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, SAP uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

- Заказчик (в том числе его Операторы) имеет доступ только к собственным данным.
- Если Персональные данные требуются для обработки инцидента сопровождения Заказчика, данные прикрепляются к такому запросу и используются только для обработки подобного запроса. Они не используются для обработки любых других запросов. Такие данные хранятся в выделенных системах сопровождения.

1.9 Контроль целостности данных Персональные данные в процессе обработки останутся неизменными, полными и актуальными.

Меры:

SAP внедрила многоуровневую стратегию защиты от несанкционированных изменений.

В частности, SAP использует следующие способы внедрения средств контроля, перечисленных в разделах о средствах контроля и мерах безопасности выше:

- Системы сетевой защиты (Firewalls);
- Центр мониторинга безопасности;
- антивирусное программное обеспечение;
- резервное копирование и восстановление данных;
- внутренние и внешние тесты на проникновение;
- регулярные независимые проверки эффективности мер безопасности.

TOMs SET 2
(applies to TOMs Set 2 Services defined above)

Last Updated: May 4, 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1. Physical Access Control.

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion

Группа ТОМ 2
(применяется к Услугам Группы ТОМ 2, определенные выше)

Последнее обновление: 4 мая, 2020

1. ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕРЫ

В следующих разделах определяются текущие технические и организационные меры SAP. SAP может менять эти меры в любой момент без уведомления при условии обеспечения аналогичного или более высокого уровня безопасности. Индивидуальные мероприятия могут быть заменены новыми мерами, если они служат той же цели и не уменьшают уровень безопасности Персональных данных.

1.1. Контроль физического доступа.

- SAP защищает свое имущество и объекты, используя соответствующие средства в соответствии с Политикой безопасности SAP
- В целом здания защищены посредством систем контроля доступа (например, системы доступа по смарт-картам).
- Минимальным требованием является оснащение внешних входов в здания сертифицированной системой ключей, обеспечивающей современное активное управление ключами.
- Могут быть реализованы дополнительные меры обеспечения безопасности зданий, отдельных территорий и прилегающих объектов с учетом классификации безопасности. Сюда относятся конкретные профили доступа, видеонаблюдение, системы тревожной сигнализации и системы биометрического контроля доступа.
- Права доступа предоставляются уполномоченным лицам на индивидуальной основе в соответствии с мерами по контролю системы и доступа к данным (см. пункты 1.2 и 1.3 ниже). Эти меры также распространяются на доступ посетителей. Гости и посетители зданий SAP обязаны зарегистрироваться на входе, сообщив свое имя, и далее следовать в сопровождении уполномоченных сотрудников компании.
- Работники SAP и сторонний персонал должны иметь при себе идентификационные карты на всех объектах SAP.

Дополнительные меры для Центров обработки данных:

- Во всех Центрах обработки данных необходимо следовать строгим процедурам безопасности с

detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

привлечением специалистов по охране и использованием камер наблюдения, детекторов движения, устройств контроля доступа и других средств, позволяющих устранить угрозы безопасности для оборудования и помещений Центра обработки данных. Только уполномоченные представители имеют доступ к системам и инфраструктуре в помещениях Центров обработки данных. В целях поддержания правильного функционирования оборудования обеспечения физической безопасности (датчиков движения, камер и т. д.) проводится регулярное обслуживание оборудования.

- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

- SAP и все сторонние провайдеры Центров обработки данных фиксируют имена и время прибытия уполномоченного персонала на закрытые территории в составе Центров обработки данных.

1.2. System Access Control.

1.2. Контроль доступа к системам.

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy

- Доступ к уязвимым системам, в том числе используемым для хранения и обработки Персональных данных, предоставляется по модели многоуровневой авторизации. Управление разрешениями осуществляется посредством определенных процессов в соответствии с Политикой безопасности SAP.

- All personnel access SAP's systems with a unique identifier (user ID).

- Весь персонал входит в системы SAP только на основании уникального идентификатора (идентификатора пользователя).

- SAP has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company, their access rights are revoked.

- В SAP действуют политики, предусматривающие, что никакие права не предоставляются без соответствующего разрешения, и если сотрудник покидает компанию, его права доступа аннулируются.

- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- В SAP действует политика паролей, запрещающая совместное использование и обмен паролями, предписывающая порядок действий в случае раскрытия пароля и устанавливающая требования о регулярной смене паролей и изменении паролей по умолчанию. Для аутентификации назначаются персональные идентификаторы пользователей. Все пароли должны соответствовать минимальным установленным требованиям и храниться в зашифрованной форме. В системе реализована принудительная смена доменных паролей каждые шесть месяцев и действуют определенные требования к сложности паролей. На каждом компьютере имеется защищенная паролем экранная заставка.

- The company network is protected from the public network by firewalls.
- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management processes to deploy relevant security updates on a regular and periodic basis.
- Full remote access to SAP's corporate network and critical infrastructure is protected by authentication.

- Сеть компании защищена от общедоступной сети брандмауэром.
- SAP использует современные антивирусные программы на точках доступа в сеть компании (для учетных записей электронной почты), а также на всех файловых серверах и всех рабочих станциях.
- Процессы управления патчами безопасности для развертывания соответствующих обновлений безопасности на регулярной и постоянной основе.
- Полный удаленный доступ к корпоративной сети и критически важной инфраструктуре SAP защищен с помощью аутентификации.

1.3. Data Access Control.

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and/or penetration tests on its IT systems.
- Processes and policies to detect the installation of unapproved software on production systems.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.3. Контроль доступа к данным

- В соответствии с Политикой безопасности SAP необходимо обеспечить защиту Персональных данных по меньшей мере на уровне защиты конфиденциальных данных в соответствии со стандартом SAP по классификации информации.
- Доступ к Персональным данным предоставляется только по служебной необходимости. Персонал имеет доступ к информации, необходимой ему для выполнения своих обязанностей. В SAP используются концепции полномочий, в рамках которых для каждой учетной записи (идентификатора пользователя) документируются процессы предоставления и назначения ролей. Все Данные заказчика защищены в соответствии с Политикой безопасности SAP.
- Все производственные серверы работают в соответствующих Центрах обработки данных или серверных помещениях. Меры безопасности, которые защищают приложения, используемые для обработки Персональных данных, регулярно проверяются. Для этого SAP проводит внутренние и внешние проверки безопасности или тесты на проникновение в свои ИТ-системы.
- Процессы и политики для выявления несанкционированной установки программного обеспечения в продуктивных системах.
- Методы уничтожения данных и носителей данных, после того как они больше не требуются, определяются правилами безопасности SAP.

1.4. Data Transmission Control.

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.

1.4. Контроль передачи данных.

- При передаче по внутренним сетям SAP Персональные данные защищаются в соответствии с Политикой безопасности SAP.

- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

- Если данные передаются между компанией SAP и Заказчиком, меры по защите передаваемых Персональных данных согласуются сторонами и включаются в соответствующее соглашение. Это условие применяется к физическому переносу данных и переносу данных по сети. В любом случае Заказчик берет на себя ответственность за любое перемещение данных за пределами подконтрольных SAP систем (например, при переносе данных за пределы брандмауэра Центра обработки данных SAP).

1.5. Data Input Control.

1.5. Контроль ввода данных.

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.

- Компания SAP разрешает доступ к Персональным данным только авторизованному персоналу, в необходимом для работы объеме.

- SAP has in most cases implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.

- Компания SAP в большинстве случаев внедрила систему регистрации ввода, изменения, удаления и блокировки Персональных данных сотрудниками SAP или ее Субподрядчиками по обработке данных в той степени, в которой это возможно в рамках предоставления Облачной услуги.

1.6. Job Control.

1.6. Контроль заданий.

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.

- Компания SAP использует средства контроля и процессы, позволяющие следить за выполнением положений договоров между SAP и ее заказчиками, субподрядчиками по обработке данных и другими поставщиками услуг.

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

- В соответствии с Политикой безопасности SAP необходимо обеспечить защиту Персональных данных по меньшей мере на уровне защиты конфиденциальных данных в соответствии со стандартом SAP по классификации информации.

- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

- Все работники, субподрядчики по обработке данных и прочие поставщики услуг SAP связаны договорными обязательствами соблюдать конфиденциальность всей уязвимой информации, включая промышленные секреты заказчиков и партнеров SAP.

1.7. Availability Control.

1.7. Контроль доступности.

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.

- SAP использует процессы регулярного резервного копирования для обеспечения возможности восстановления критически важных бизнес-систем по мере необходимости.

- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.

- SAP использует источники бесперебойного питания (например, ИБП, аккумуляторы, генераторы и т. д.), чтобы поддержать непрерывную работу систем электропитания Центров обработки данных.

- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8. Data Separation Control.

- SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9. Data Integrity Control.

- SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, SAP uses the following to implement the control and measure sections described above.
- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing and/or regular external audits to prove security measures.

- Компания SAP определила планы для внештатных ситуаций в связи с критически важными для бизнеса процессами и может предложить стратегии аварийного восстановления критически важных для бизнеса служб, подробно описанные в Документации или включенные в Договор для соответствующей Облачной услуги.
- Регулярно проводятся испытания аварийных процессов и систем.

1.8. Контроль разделения данных.

- SAP использует технические возможности развернутого программного обеспечения (например, многопользовательские или раздельные системные ландшафты) для разделения Персональных данных от разных заказчиков.
- Заказчик (в том числе его Операторы) имеет доступ только к собственным данным.
- Если Персональные данные требуются для обработки инцидента сопровождения Заказчика, данные прикрепляются к такому запросу и используются только для обработки подобного запроса. Они не используются для обработки любых других запросов. Такие данные хранятся в выделенных системах сопровождения.

1.9. Контроль целостности данных.

- SAP внедрила многоуровневую стратегию защиты от несанкционированных изменений.
- В частности, SAP использует следующее для реализации контроля и внедрения мер, описанных выше.
- Системы сетевой защиты (Firewalls);
- Центр мониторинга безопасности;
- Антивирусное программное обеспечение;
- Резервное копирование и восстановление данных;
- Внешние и внутренние тесты на проникновение или регулярные независимые проверки эффективности мер безопасности.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Приложение 3 к Соглашению об обработке персональных данных и, если применимо, Стандартным договорным условиям

В следующей таблице изложены соответствующие статьи GDPR и соответствующие условия Соглашения об обработке персональных данных. Здесь они приведены исключительно в иллюстративных целях.

Article of GDPR **Статья GDPR**	**Section of DPA** **Раздел Соглашения об обработке персональных данных**	**Click on link to see Section** **Пройдите по ссылке, чтобы просмотреть раздел**
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(1)	2 и Приложение 2	Security of Processing и Приложение 2 «Технические и организационные меры».
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28(2), 28(3) (d) и 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application. Structure.
28(3) предложение 1	1.1 и Приложение 1, 1.2	Purpose and Application. Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (a) и 29	3.1 и 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (c) и 32	2 и Приложение 2	Security of Processing и Приложение 2 «Технические и организационные меры».
28(3) (e)	3.4	Cooperation.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach. Notification Data Protection Impact Assessment.
28(3) (f) и 32–36	2 и Приложение 2, 3.5, 3.6	Security of Processing и Приложение 2 «Технические и организационные меры». Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion
28(3) (g)	4	Data export and Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
28(4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
30	8	Documentation; Records of processing

46(2) (c)	7.2	Standard Contractual Clauses.
46(2) (c)	7.2	Standard Contractual Clauses.

Appendix 4

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer also on behalf of the other Controllers

(in the Clauses hereinafter referred to as the '**data exporter'**)

and

SAP

(in the Clauses hereinafter referred to as the **'data importer'**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

Приложение 4

СТАНДАРТНЫЕ ДОГОВОРНЫЕ УСЛОВИЯ (ОБРАБОТЧИКИ)[2]

Для целей статьи 26(2) Директивы 95/46/EC (а начиная с 25 мая 2018 года статьи 44 и далее Регламента 2016/79) для передачи персональных данных обработчикам, учрежденным в третьих странах, в которых не обеспечен должный уровень защиты данных

Заказчик, в том числе от имени других Операторов

(в настоящих Условиях, далее именуемый «**экспортером данных»**),

и

SAP

(в настоящих Условиях, далее именуемый «**импортером данных»**)

(каждый из них именуется по отдельности «сторона», а совместно — «стороны»)

ДОГОВОРИЛИСЬ о следующих Договорных условиях («Условия») с целью принять надлежащие меры для защиты права на неприкосновенность частной жизни и основных прав и свобод граждан в связи с передачей персональных данных, указанных в Дополнении 1, от экспортера данных импортеру данных.

Пункт 1.

Определения

В контексте настоящих Условий:

(a) термины «персональные данные», «особые категории данных», «обрабатывать/обработка», «оператор персональных данных», «обработчик», «субъект данных» и «надзорный орган» имеют значения, предусмотренные в Директиве 95/46/EC Европейского парламента и Совета от 24 октября 1995 года о защите физических лиц в связи с обработкой персональных данных и о свободном передвижении таких данных;

(b) «экспортер данных» означает оператора персональных данных, осуществляющего их передачу;

(c) «импортер данных» означает обработчика, который соглашается получить от экспортера данных персональные данные, предназначенные для обработки по поручению экспортера данных после передачи в соответствии с его поручениями и положениями Условий, и действия которого не регулируются системой третьей страны, обеспечивающей должный уровень защиты согласно статье 25(1) Директивы 95/46/EC;

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

[2] В соответствии с Решением Комиссии от 5 февраля 2010 года (2010/87/EU)

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(d) «субподрядчик по обработке» означает любого обработчика, привлекаемого импортером данных или другим субподрядчиком по обработке импортера данных, который соглашается получить от импортера данных или его другого субподрядчика по обработке персональные данные, которые предназначены исключительно для обработки, выполняемой по поручению экспортера данных после передачи в соответствии с его поручениями, положениями Условий и письменным договором субподряда;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(e) «применимое законодательство о защите данных» означает законодательство, защищающее фундаментальные права и свободы человека, в частности право на неприкосновенность частной жизни в связи с обработкой Персональных данных, и применяемое к оператору персональных данных в Государстве-члене, в котором находится экспортер данных;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

(f) «технические и организационные меры по обеспечению безопасности» означают меры, нацеленные на защиту персональных данных от случайного или незаконного уничтожения, потери, изменения, несанкционированного раскрытия или доступа, в частности в случаях, когда обработка предполагает передачу данных по сети, а также от всех остальных форм незаконной обработки.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Пункт 2.

Сведения о передаче данных

Подробные сведения о передаче, в частности, применимые особые категории персональных данных, указаны в Дополнении 1, составляющем неотъемлемую часть Условий.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

Пункт 3.

Условие о стороннем бенефициаре

1. Субъект данных может в качестве стороннего бенефициара потребовать принудительного исполнения экспортером данных условий настоящего пункта, пунктов 4(b)–(i), пунктов 5(a)–(e) и (g)–(j), пунктов 6(1) и (2), пункта 7, пункта 8(2) и пунктов 9–12.

2. Субъект данных может потребовать принудительного исполнения импортером данных условий настоящего пункта, пунктов 5(a)–(e) и (g), пункта 6, пункта 7, пункта 8(2) и пунктов 9–12, если экспортер данных фактически исчез или прекратил юридическое существование, кроме случаев, когда организация-преемник взяла на себя все юридические обязательства экспортера данных на основании договора или закона, в результате чего эта организация приобретает права и обязательства экспортера данных и, следовательно, субъект

данных может потребовать их исполнения от этой организации.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. Субъект данных может потребовать принудительного исполнения субподрядчиком по обработке условий настоящего пункта, пунктов 5(a)–(e) и (g), пункта 6, пункта 7, пункта 8(2) и пунктов 9–12, если экспортер данных и импортер данных фактически исчезли или прекратили юридическое существование, кроме случаев, когда организация-преемник взяла на себя все юридические обязательства экспортера данных на основании договора или закона, в результате чего эта организация приобретает права и обязательства экспортера данных и, следовательно, субъект данных может потребовать их исполнения от этой организации. Ответственность субподрядчика по обработке перед третьими лицами ограничивается его собственными операциями по обработке согласно Условиям.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Стороны не возражают против того, чтобы интересы субъекта данных представлялись ассоциацией или другим органом, если субъект данных явным образом выразит в этом желание и если это не запрещено национальным законодательством.

Clause 4

Obligations of the data exporter

Пункт 4.

Обязательства экспортера данных

The data exporter agrees and warrants:

Экспортер данных подтверждает и гарантирует, что:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(a) Обработка персональных данных, включая их передачу, выполняется и будет выполняться согласно соответствующим положениям применимого законодательства о защите персональных данных (и, где это применимо, о ней уведомлены соответствующие органы Государства-члена, в котором расположен экспортер данных) и не нарушает соответствующих законов этого государства;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(b) он дал и на протяжении всего периода предоставления услуг обработки персональных данных будет продолжать давать импортеру данных указания, что обработке подлежат только персональные данные, переданные в интересах экспортера данных, и обработку следует выполнять только в соответствии с действующим законодательством о защите данных и Условиями;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(c) импортер данных предоставит достаточные гарантии в отношении технических и организационных мер по обеспечению безопасности, указанных в Приложении 2 к настоящему договору;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these

(d) после оценки требований применимого законодательства о защите данных меры безопасности соответствуют уровню, необходимому для защиты персональных данных от случайного или незаконного уничтожения или потери, изменения, несанкционированного раскрытия и использования, в частности, когда обработка предполагает передачу данных по сети, а также от любых других

measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

незаконных форм обработки, и что эти меры обеспечивают уровень безопасности, соответствующий рискам, возникающим при обработке, и характеру защищаемых данных, с учетом уровня технологий и стоимости их реализации;

(e) that it will ensure compliance with the security measures;

(e) он обеспечит соблюдение мер безопасности;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(f) если передача касается специальных категорий данных, субъект данных проинформирован или будет проинформирован до передачи или как можно скорее после нее о том, что его данные могут быть переданы в другую страну, не обеспечивающую должный уровень защиты согласно Директиве 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(g) он будет передавать любые уведомления, полученные от импортера данных или субподрядчика по обработке согласно пунктам 5(b) и 8(3), надзорному органу по защите данных, если экспортер данных решит продолжить передачу или отменить приостановку;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(h) он по запросу предоставит субъектам данных копию Условий, за исключением Приложения 2, а также сводное описание мер безопасности и копию любого договора о субподряде услуг обработки данных, заключаемого в соответствии с Условиями, за исключением случаев, когда Условия или договор субподряда содержат коммерческую информацию; при наличии такой коммерческой информации в Условиях или договоре субподряда импортер данных может удалить ее;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(i) в случае субподряда процедура обработки данных будет выполняться в соответствии с пунктом 11 субподрядчиком по обработке, обеспечивающим как минимум такой же уровень защиты персональных данных и прав субъекта данных, что и импортер данных, действующий в соответствии с Условиями;

(j) that it will ensure compliance with Clause 4(a) to (i).

(j) он обеспечит выполнение пунктов 4(a)–(i).

Clause 5

Obligations of the data importer

Пункт 5.

Обязательства импортера данных

The data importer agrees and warrants:

Импортер данных подтверждает и гарантирует, что:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(a) он будет выполнять обработку персональных данных только по поручению экспортера данных и в соответствии с его указаниями и Условиями; если импортер данных не сможет по каким-либо причинам обеспечить такое соответствие, он обязуется сообщить об этом экспортеру данных в кратчайший срок, и в этом случае экспортер данных имеет право приостановить передачу данных и (или) прекратить действие договора;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial

(b) у него нет причин полагать, что применимое к нему законодательство не позволяет ему выполнять поручения, получаемые от экспортера данных, и его обязательства в соответствии с договором, и если изменение этого законодательства окажет

adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

значительное отрицательное влияние на возможность импортера данных выполнять свои гарантии и обязательства, изложенные в Условиях, то он немедленно уведомит о таком изменении экспортера данных, как только о нем узнает, и в этом случае экспортер данных имеет право приостановить передачу данных и (или) прекратить действие договора;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(c) перед обработкой переданных персональных данных будут реализованы все технические и организационные меры по обеспечению безопасности, указанные в Приложении 2;

(d) that it will promptly notify the data exporter about:

(d) он незамедлительно уведомит экспортера данных о:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(i) любом юридически обязывающем запросе на раскрытие персональных данных, полученном от правоохранительного органа, за исключением случаев, когда это запрещено, например в случае требования о сохранении конфиденциальности проводимого правоохранительным органом расследования согласно уголовному законодательству;

(ii) any accidental or unauthorised access; and

(ii) любом случайном или несанкционированном доступе к данным;

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(iii) любом запросе, напрямую полученном от субъектов данных, не отвечая на этот запрос, кроме случаев, когда ответ на запрос санкционирован;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(e) он немедленно и должным образом будет отвечать на запросы экспортера, касающиеся обработки Персональных данных, подлежащих передаче, и придерживаться рекомендаций надзорного органа относительно обработки переданных данных;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(f) по запросу экспортера данных он предоставит свои помещения, в которых выполняется обработка данных, для аудита операций по обработке, описанного в Условиях и выполняемого экспортером данных либо органом проверки, состоящим из независимых лиц, которые обладают необходимыми профессиональными качествами, связаны требованиями конфиденциальности и выбираются экспортером данных, где это применимо, по согласованию с надзорным органом;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(g) по запросу он предоставит субъекту данных копию Условий или любого существующего договора о субподряде услуг обработки данных, за исключением случаев, когда эти Условия или договор содержат коммерческую информацию, которую в таком случае он может удалить, кроме Приложения 2, которое будет заменено сводным описанием мер безопасности в тех случаях, когда субъект данных не может получить копию от экспортера данных;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(h) в случае передачи обработки данных на субподряд он предварительно уведомит об этом экспортера данных и получит его письменное согласие;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

(i) субподрядчик по обработке будет оказывать услуги обработки в соответствии с пунктом 11;

(j) он незамедлительно отправит экспортеру данных копию любого соглашения, заключенного с субподрядчиком обработки данных в соответствии с Условиями.

Clause 6

Liability

Пункт 6.

Ответственность

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

1. Стороны соглашаются с тем, что любой субъект данных, понесший ущерб в результате нарушения обязательств, указанных в пунктах 3 или 11 любой из сторон или субподрядчиком по обработке, имеет право на получение от экспортера данных компенсации понесенного ущерба.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

2. Если субъект данных не может предъявить экспортеру данных требование о компенсации согласно подпункту 1 в связи с нарушением импортером данных или его субподрядчиком по обработке какого-либо из обязательств, описанных в пункте 3 или 11, поскольку экспортер данных фактически исчез, прекратил юридическое существование или обанкротился, импортер данных признает, что субъект данных может предъявить импортеру данных требование о компенсации, как если бы тот был экспортером данных, кроме случаев, когда организация-преемник взяла на себя все юридические обязательства экспортера на основании договора или закона, и в этом случае субъект данных может потребовать от этой организации принудительной реализации своих прав.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

Импортер данных не может уклониться от ответственности по своим обязательствам, ссылаясь на нарушение обязательств субподрядчиком по обработке.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. Если субъект данных не может предъявить экспортеру или импортеру данных требование о компенсации согласно подпункту 1 и 2 в связи с нарушением субподрядчиком по обработке какого-либо из обязательств, описанных в пункте 3 или 11, поскольку экспортер и импортер данных фактически исчезли, прекратили юридическое существование или обанкротились, субподрядчик по обработке признает, что субъект данных может предъявить субподрядчику по обработке требование о компенсации, как если бы тот был экспортером или импортером данных, применительно только к операциям обработки, выполненным субподрядчиком, кроме случаев, когда организация-преемник взяла на себя все юридические обязательства экспортера или импортера данных на основании договора или закона, и в этом случае субъект данных может потребовать от этой организации принудительной реализации своих прав. Ответственность субподрядчика по обработке данных ограничивается его собственными операциями по обработке, выполняемыми согласно Условиям.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Пункт 7.

Посредничество и юрисдикция

1. Импортер данных признает, что, если субъект данных применит против него права стороннего бенефициара и (или) предъявит требование о компенсации ущерба согласно Условиям, импортер данных согласится с решением субъекта данных:

   (a) о разрешении спора путем посредничества независимого лица или, где это применимо, надзорного органа;

   (b) о передаче спора в суд Государства-члена, в котором расположен экспортер данных.

2. Стороны соглашаются с тем, что выбор, сделанный субъектом данных, не нанесет ущерба его материальным и процессуальным правам на меры защиты согласно другим положениям национального или международного законодательства.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Пункт 8.

Сотрудничество с надзорными органами

1. Экспортер данных согласен предоставить копию настоящего договора надзорному органу по запросу или в соответствии с требованием применимого законодательства о защите данных.

2. Стороны признают, что надзорный орган имеет право проводить аудит импортера данных и любого субподрядчика по обработке. Объем аудита и его условия совпадают с объемом и условиями аудита, который проводился бы экспортером данных согласно применимому законодательству о защите данных.

3. Импортер данных в кратчайший срок сообщит экспортеру данных о наличии закона, который распространяется на него или любого субподрядчика по обработке и не позволяет проводить аудит импортера данных или любого субподрядчика по обработке в соответствии с подпунктом 2. В этом случае экспортер и импортер данных имеют право принять меры, предусмотренные в пункте 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Пункт 9.

Применимое законодательство

Условия регулируются законодательством Государства-члена, в котором зарегистрирован Экспортер данных.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Пункт 10.

Изменения договора

Стороны обязуются не вносить изменения в Условия. Это не запрещает сторонам при необходимости добавлять пункты, связанные с бизнесом и не противоречащие Условиям.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Пункт 11.

Передача услуг обработки данных на субподряд

1. Без предварительного письменного согласия экспортера данных импортер данных не имеет права передавать на субподряд какие-либо операции по обработке данных, выполняемые по поручению экспортера данных согласно Условиям. В тех случаях, когда с согласия экспортера данных импортер данных передает выполнение своих обязательств, предусмотренных Условиями, на субподряд, он обязуется делать это только при условии заключения письменного соглашения с субподрядчиком по обработке, которое налагает на субподрядчика по обработке те же обязательства, чтоб берет на себя импортер данных согласно Условиям. Если субподрядчик по обработке не выполняет обязательства по защите данных, предусмотренные таким письменным соглашением, импортер данных несет полную ответственность перед экспортером данных за исполнение обязательств субподрядчика по обработке по указанному соглашению.

2. Предварительный письменный договор между импортером данных и субподрядчиком по обработке также должен включать условие о стороннем бенефициаре, аналогичное положениям пункта 3, применительно к случаям, когда субъект данных не может предъявить экспортеру или импортеру данных требование о компенсации, упомянутое в подпункте 1 пункта 6, поскольку экспортер и импортер данных фактически исчезли, прекратили юридическое существование или обанкротились и нет организации-преемника, которая взяла бы на себя все юридические обязательства экспортера или импортера данных на основании договора или закона. Ответственность субподрядчика по обработке перед третьими лицами ограничивается его собственными операциями по обработке согласно Условиям.

3. Положения, касающиеся аспектов защиты данных при передаче обработки данных на субподряд в соответствии с подпунктом 1, регулируются в соответствии с законодательством Государства-члена, в котором учрежден экспортер данных.

4. Экспортер данных ведет перечень соглашений о субподряде, которые были заключены в соответствии с Условиями и о которых импортер данных уведомил его в соответствии с пунктом 5(j). Актуальность этого списка должна проверяться не менее одного раза в год. Список должен быть доступен надзорному органу по защите данных, контролирующему деятельность экспортера данных.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer

Пункт 12.

Обязательства после прекращения услуг обработки персональных данных

1. Стороны соглашаются, что после прекращения оказания услуг обработки данных импортер данных

and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

и субподрядчик по обработке в зависимости от решения экспортера данных либо вернут все переданные персональные данные и их копии экспортеру данных, либо уничтожат все персональные данные и предоставят экспортеру данных подтверждение этого, за исключением случаев, когда законодательство, применяемое к импортеру данных, не разрешает возврат или уничтожение всех переданных персональных данных или любой их части. В этом случае импортер данных обязуется обеспечить конфиденциальность переданных персональных данных и прекратить их активную обработку.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

2. Импортер данных и субподрядчик по обработке обязуются по запросу экспортера данных и (или) надзорного органа предоставить свои помещения по обработке данных для проверки мер, описанных в подпункте 1.