ПРИЛОЖЕНИЕ ПО ОБРАБОТКЕ ДАННЫХ IVANTI

Настоящее Приложение по обработке данных Ivanti («ПОД») является частью Лицензионного соглашения с конечным пользователем и соглашения на обслуживание компании Ivanti («Соглашение»), составлено и вступает в силу с даты подписания последней из сторон («Дата вступления в силу»), указанной ниже, между заказчиком, указанным ниже или в Соглашении («Контролер»), и соответствующем юридическим лицом Ivanti, указанным в настоящем ПОД («Ivanti» или «Обработчик») (по отдельности «Сторона»; вместе «Стороны»). Любые термины, написанные с заглавной буквы, не определенные в настоящем документе, имеют соответствующие значения, данные им в Соглашении.

ПРЕАМБУЛА

ПРИНИМАЯ ВО ВНИМАНИЕ, что Стороны заключили Соглашение.

ПРИНИМАЯ ВО ВНИМАНИЕ, что в ходе предоставления Услуг Контролеру в соответствии с Соглашением Обработчик может Обрабатывать Персональные данные от имени Контролера;

ПРИНИМАЯ ВО ВНИМАНИЕ, что для обеспечения надлежащих мер безопасности в отношении Обработки Персональных данных, предоставляемых Контролером Обработчику, Стороны соглашаются соблюдать следующие положения в отношении любых Персональных данных, каждая из которых действует в соответствии с объективной необходимостью и добросовестно.

ТАКИМ ОБРАЗОМ, принимая во внимание вышеизложенные предпосылки и взаимные обещания и соглашения, изложенные ниже, Контролер и Обработчик настоящим соглашаются о нижеследующем:

СОГЛАШЕНИЕ

1. ОПРЕДЕЛЕНИЯ

Все термины, написанные с заглавной буквы, не определенные в настоящем документе, имеют значение, указанное в Соглашении.

«Аффилированное лицо» означает любую организацию, которая прямо или косвенно контролирует, контролируется или находится под общим контролем с субъектом. «Контроль» для целей данного определения означает прямое или косвенное владение или контроль над более чем 50% голосующих акций субъекта.

«**Применимые законы о защите данных**» означает все применимые законы, нормативные акты, нормативные руководства или требования в любой юрисдикции, касающиеся защиты данных, неприкосновенности частной жизни или конфиденциальности Персональных данных, включая, помимо прочего, (a) GDPR вместе с любым транспонирующим, имплементирующим или дополнительным законодательством, а также (b) CCPA.

«Уполномоченное аффилированное лицо» означает любое из аффилированных лиц Контролера, которые (a) подпадают под действие законов и правил о защите данных Европейской экономической зоны и/или ее государств-членов, Соединенного Королевства и Швейцарии, (b) подпадают под действие законов и правил о защите данных за пределами Европейской экономической зоны и/или ее государств-членов, Швейцарии и Соединенного Королевства (в зависимости от обстоятельств) и (c) разрешили использовать Обработчик для обработки данных в соответствии с Соглашением.

«CCPA» означает Калифорнийский закон о конфиденциальности потребителей, Гражданский Кодекс Калифорнии § 1798.100 *и последующие*, а также правила его реализации.

«Контролер» означает лицо, которое определяет цели и средства Обработки Персональных данных. Во избежание сомнений, Сторона, указанная выше как «Контролер», является Контролером в рамках настоящего ПОД.

«Утечка данных» означает нарушение безопасности, ведущее к случайному, несанкционированному или незаконному уничтожению, потере, изменению, раскрытию, доступу или другой обработке Персональных данных, передаваемых, хранимых или Обрабатываемых иным образом.

«Орган по защите данных» означает любого представителя или агента государственного органа или агентства, который уполномочен обеспечивать соблюдение Применимых законов о защите данных.

«Субъект данных» означает физическое лицо, к которому относятся Персональные данные.

«GDPR» означает Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отменяющий Директиву 95/46/ЕС (Общий регламент по защите данных).

«Ivanti» означает юридическое лицо, указанное ниже, в том же географическом регионе, что и Заказчик:

- Ivanti, Inc., корпорация штата Делавэр, в Северной и Южной Америке, кроме Бразилии.
- Ivanti Comércio de Software Brasil Ltda, бразильская компания в Бразилии.
- Ivanti Software K.K., японская компания в Японии.
- Ivanti Software Technology (Beijing) Co., Ltd., китайская компания в Китае.
- Ivanti International Limited, ирландская компания, для продуктов и услуг под брендами Wavelink и Naurtech в Европе, на Ближнем Востоке, в Африке и Азиатско-Тихоокеанском регионе.
- Ivanti UK Limited, компания с ограниченной ответственностью, зарегистрированная в Англии и Уэльсе, во всех других местоположениях.

«Персональные данные» означают любую информацию, которая идентифицирует, относится, описывает, может быть связана или может быть обоснованно связана, прямо или косвенно, с идентифицированным или идентифицируемым физическим лицом или конкретным домохозяйством. Идентифицируемое физическое лицо — это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на такой идентификатор, как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или на один или несколько факторов, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.

«Обработка» означает любую операцию или набор операций, которые выполняются с Персональными данными посредством или в связи с предоставлением Услуг, независимо от того, выполняются ли они с помощью автоматических средств, таких как сбор, запись, организация, хранение, адаптация или изменение, получение, консультация, использование, раскрытие путем передачи, распространения или иного предоставления, разглашение или комбинирование, блокирование, стирание или уничтожение; и как определено Применимыми законами о защите данных.

«Обработчик» означает юридическое лицо, которое обрабатывает Персональные данные от имени Контролера. Во избежание сомнений, Сторона, указанная выше как «Обработчик», является Обработчиком данных ПОД.

«Услуги» означает Обработку Персональных данных Обработчиком в связи и в целях предоставления услуг, которые должны предоставляться Обработчиком в соответствии с Соглашением.

«Поставщик услуг» означает индивидуальное предприятие, товарищество, компанию с ограниченной ответственностью, корпорацию, ассоциацию или другое юридическое лицо, которое организовано или действует для получения прибыли или финансовой выгоды своих акционеров или других владельцев, которые обрабатывают информацию от имени Контролера данных и которым Контролер данных раскрывает Персональные данные Субъекта данных в коммерческих целях в соответствии с письменным договором, при условии, что договор запрещает Поставщику услуг сохранять, использовать или раскрывать Персональные данные для любых целей, кроме конкретной цели оказания услуг, указанных в договоре, или иным образом разрешенным CCPA, включая сохранение, использование или раскрытие Персональных данных в Коммерческих целях, кроме предоставления услуг, указанных в договоре с Контролером данных. Термины «Деловая цель» и «Коммерческая цель» имеют то же значение, что и эти термины, используемые в CCPA. Во избежание сомнений, Обработчик является Поставщиком услуг.

«Субобработчик» означает любую организацию, которая обрабатывает Персональные данные от имени Обработчика.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Роли Сторон. Стороны признают и соглашаются с тем, что в отношении Обработки Персональных данных Контролер — это Контролер, Обработчик — это Обработчик или Поставщик услуг. Предмет, продолжительность, цель Обработки, а также типы Персональных данных и категории Субъектов данных, обрабатываемых в рамках настоящего ПОД, дополнительно указаны в Приложении 1.

2.2 Обязанности Контролера. Инструкции Контролера по обработке Персональных данных должны соответствовать Законам и правилам о защите данных. Контролер несет единоличную ответственность за точность, качество и законность Персональных данных, а также за средства, с помощью которых Контролер получает Персональные данные и предоставляет их Обработчику.

2.3 Обязанности Обработчика. Все Персональные данные, обрабатываемые Обработчиком в соответствии с Соглашением, являются Конфиденциальной информацией, и Обработчик будет обрабатывать Персональные данные только в соответствии с документированными инструкциями Контроллера, изложенными в Приложении 1, или иным образом предоставленными Контролером в письменной форме. Обработчик не будет продавать Персональные данные, обрабатываемые в соответствии с настоящим ПОД, и не будет хранить, использовать или раскрывать Персональные данные за рамками прямых деловых отношений между Обработчиком и Контролером. Обработчик должен соблюдать все Применимые законы о защите данных в отношении обработки Персональных данных. Если Обработчик считает, что выполнение каких-либо инструкций Контролера приведет к нарушению любого Применимого законодательства о защите данных, Обработчик должен незамедлительно уведомить об этом Контролера в письменной форме. Обработчик должен предоставить Контролеру всю информацию, необходимую для демонстрации соблюдения Обработчиком своих обязательств по настоящему ПОД.

2.3.1. Требования по оказанию помощи. Обработчик должен помочь Контролеру: соблюдать Применимое законодательство о защите данных; предполагаемые и соответствующие нарушения данных; уведомления или запросы от органа по защите данных; уведомления и запросы от субъектов данных; и обязанность Контролера проводить оценку воздействия на защиту данных и предварительные консультации с Органом по защите данных.

3. ОБЯЗАТЕЛЬСТВА ПО УВЕДОМЛЕНИЮ

3.1 Обязательства Обработчика по уведомлению. Обработчик должен немедленно уведомить Контролера в письменной форме о следующем:

3.1.1 Запрос Субъекта данных об осуществлении своих прав на конфиденциальность, таких как доступ, исправление, удаление, транспортировка, возражение или ограничение его Персональных данных;

3.1.2 Любой запрос или жалоба, полученные от заказчиков или сотрудников Контролера;

3.1.3 Любой вопрос, жалоба, расследование или другой запрос от Органа по защите данных;

3.1.4 Любой запрос на раскрытие Персональных данных, который каким-либо образом связан с Обработкой Персональных данных Обработчиком в рамках настоящего ПОД;

3.1.5 Утечка данных в соответствии с обязательствами по уведомлению, изложенными в Разделе 7.1; а также

3.1.6 Когда Персональные данные становятся предметом обыска и изъятия, судебного приказа о наложении ареста, конфискации в ходе процедуры банкротства или несостоятельности или аналогичных действий или мер со стороны третьих лиц во время их Обработки.

Обработчик будет помогать Контролеру в выполнении обязательств Контролера по ответу на запросы, относящиеся к пунктам (3.1.1) - (3.1.6) выше, и не будет отвечать на такие запросы без предварительного письменного согласия Контролера, за исключением случаев, когда ответственность от Обработчика требуется по закону.

3. КОНФИДЕНЦИАЛЬНОСТЬ

4.1 Конфиденциальная информация. Вся информация, предоставляемая Обработчику данных в соответствии с Соглашением, является Конфиденциальной информацией.

4.2 Персонал Обработчика. Обработчик должен обеспечить, чтобы его персонал, занимающийся обработкой Персональных данных, был проинформирован о конфиденциальном характере Персональных данных, прошел соответствующее обучение по своим обязанностям и подписал письменные соглашения о конфиденциальности. Обработчик должен обеспечить, чтобы такие обязательства по конфиденциальности оставались в силе после прекращения соответствующих трудовых отношений с такими лицами.

4.3 Ограничение доступа. Обработчик должен обеспечить, чтобы доступ Обработчика к Персональным данным был ограничен тем персоналом, который оказывает Услуги в соответствии с Соглашением.

5. СУБОБРАБОТЧИКИ

5.1 Назначение Субобработчиков. Контролер признает и соглашается с тем, что Обработчик и Аффилированные лица Обработчика могут привлекать сторонних Субобработчиков в связи с предоставлением Услуг. Обработчик или Аффилированное лицо обработчика должно заключить письменное соглашение с каждым Субобработчиком, содержащее обязательства по защите данных, не меньшей эффективности, чем те, которые предусмотрены в настоящем ПОД, в той мере, в какой это применимо к характеру Услуг, предоставляемых таким Субобработчиком. Настоящим Контролер уполномочивает Обработчика задействовать свой текущий список Субобработчиков, указанный на странице https://www.ivanti.com/company/legal/ivanti-subprocessors, для обработки Персональных данных в соответствии с настоящим ПОД. Контролер не будет напрямую связываться с Субобработчиками Обработчика по поводу Услуг, если только Обработчик не даст на это согласие по своему собственному усмотрению.

5.2 Уведомление об изменении Субобработчиков. Обработчик будет информировать Контролера о любых предполагаемых изменениях, касающихся добавления или замены Субобработчиков, предоставив Контроллеру механизм подписки на уведомления о новых Субобработчиках по адресу https://www.ivanti.com/company/legal/ivanti-subprocessors. Обработчик уведомит Контролера о любых предполагаемых изменениях, касающихся добавления или замены Субобработчиков, до использования Субобработчика.

5.3 Право на возражение в отношении новых Субобработчиков. Контролер может обоснованно возражать против использования Обработчиком нового Субобработчика, незамедлительно уведомив обработчика в письменной форме в течение пятнадцати (15) рабочих дней после получения уведомления от Обработчика. В случае, если Контролер возражает против нового Субобработчика, Обработчик приложит разумные усилия, чтобы сделать доступным для Контролера изменение в Услугах, чтобы избежать Обработки Персональных данных новым Субобработчиком, против которого возражают. Если Обработчик не может внести такое изменение, Контролер может расторгнуть применимое Соглашение в отношении тех Услуг, которые не могут быть предоставлены Обработчиком без использования нового Субобработчика, против которого возражают.

5.4 Ответственность за действия Субобработчиков. Обработчик несет ответственность за действия и бездействие своих Субобработчиков в той же степени, в которой Обработчик несет ответственность, если бы он предоставлял услуги каждому Субобработчику непосредственно в соответствии с условиями настоящего ПОД.

6. БЕЗОПАСНОСТЬ

6.1 Защита персональных данных. Обработчик должен поддерживать соответствующие технические и организационные меры для защиты безопасности (включая защиту от несанкционированной или незаконной Обработки и от случайного или незаконного уничтожения, потери, изменения или повреждения, несанкционированного раскрытия или доступа к Персональным данным), конфиденциальности и целостности Персональных данных.

6.2 Права на аудит. Контролер соглашается, что его право на аудит Обработчика может быть удовлетворено предоставлением Обработчиком актуальных подтверждений, отчетов или выписок из независимых органов, включая, помимо прочего, внешних или внутренних аудиторов, сотрудника по защите данных Обработчика, отдел ИТ-безопасности, защиту данных или аудиторов качества или другое взаимно согласованное с третьими сторонами или сертификацию в виде аудита ИТ-безопасности или защиты данных. В той мере, в какой невозможно выполнить аудиторское обязательство, предусмотренное применимыми законами и положениями о защите данных, посредством таких аттестаций, отчетов или выписок, Контролер или назначенное им лицо имеет право проводить аудит и инспектировать — за счет Контролера — помещения, политики, процедуры и компьютеризированные системы Обработчика, чтобы убедиться, что Обработчик соответствует требованиям настоящего ПОД. Контролер или назначенное им лицо уведомит об этом не менее чем за 30 (тридцать) дней до проведения аудита, за исключением случаев, когда такой аудит требуется из-за Утечки данных с участием Обработчика данных. Аудиты, проводимые Контролером или уполномоченным им лицом, не нарушают обязательства Обработчика в отношении конфиденциальности перед другими клиентами Обработчика. Все виды аудита будут проводиться в обычное рабочее время в основном офисе Обработчика или в другом месте(ах) Обработчика, где осуществляется доступ, обработка или управление Персональными данными, и они не будут необоснованно мешать повседневной деятельности Обработчика. Перед началом любого такого аудита Обработчик и Контролер должны взаимно согласовать сроки, объем и

продолжительность аудита. Контролер может запросить краткий отчет(ы) об аудите или проводить аудит Обработчика не чаще одного раза в год.

7. УТЕЧКА ДАННЫХ

7.1 Уведомление об утечке данных. Обработчик должен уведомить Контролера в письменной форме без неоправданной задержки после того, как ему станет известно о предполагаемой Утечке данных. Ни в коем случае такое уведомление не должно быть сделано позднее, чем через 72 часа после обнаружения Обработчиком утечки данных.

7.2 Управление утечкой данных. Обработчик должен приложить разумные усилия для выявления причины такой Утечки данных и предпринять те шаги, которые Обработчик сочтет необходимыми и разумными для устранения причины такой Утечки данных в той мере, в какой устранение находится в пределах разумного контроля Обработчика.

8. ПРЕКРАЩЕНИЕ

8.1 Прекращение. Действие настоящего ПОД прекращается автоматически в случае (a) расторжения или истечения срока действия Соглашения или (b) удаления или возврата Обработчиком Персональных данных в зависимости от того, что произойдет позже. Кроме того, Контролер имеет право прекратить действие настоящего ПОД по причине, если Обработчик, по единоличному мнению Контролера, совершает существенное или постоянное нарушение настоящего ПОД, которое, в случае нарушения, поддающегося устранению, не должно быть устранено в течение десяти (10) дней с даты получения Обработчиком уведомления от Контролера, в котором указывается нарушение и запрашивается его устранение.

8.2 Возврат или удаление данных. После прекращения действия настоящего ПОД Обработчик удалит или вернет все существующие копии Персональных данных, если применимое законодательство не требует дальнейшего хранения Персональных данных. По запросу Контролера Обработчик должен подтвердить соблюдение таких обязательств в письменной форме и удалить все существующие копии. В случаях, когда местное законодательство требует, чтобы Обработчик сохранял Персональные данные, Обработчик будет защищать конфиденциальность, целостность и доступность Персональных данных; не будет активно обрабатывать Персональные данные; и будет продолжать соблюдать условия настоящего ПОД.

9. МЕХАНИЗМЫ МЕЖДУНАРОДНЫХ ПЕРЕДАЧ

9.1 Передача за пределы ЕС. В ходе предоставления Услуг в соответствии с ПОД Контроллеру может потребоваться передать Персональные данные из Европейского Союза, Европейской экономической зоны и/или их государств-членов, Швейцарии или Соединенного Королевства Обработчику в стране, которая не имеет решения о достаточности от Европейской комиссии или не находится в Европейской экономической зоне.

9.1.1. В отношении Персональных данных, подпадающих под действие GDPR (i) Обработчик будет считаться «импортером данных», а Контролер — «экспортером данных»; (ii) условия Модуля 2 применяются, если Контроллер является Контроллером данных, а Обработчик является Обработчиком данных; (iii) в Пункте 7 необязательная стыковочная оговорка должна быть удалена; (iv) в Пункте 9 Модуля 2 применяется Вариант 2, а список Субобработчиков и период времени для уведомления об изменениях должен быть согласован в Разделе 5 настоящего ПОД; (v) в Пункте 11 факультативная формулировка должна быть удалена; (vi) в Пункте 17 применяется Вариант 1, а Стандартные договорные положения регулируются государством-членом, в котором находится Контролер; (vii) в Пункте 18(b) споры должны разрешаться в судах государства-члена, где проживает Контролер; (viii) Приложение I и Приложение II считаются дополненными информацией, изложенной в Приложении 1 настоящего ПОД соответственно; и (ix) если Стандартные пункты договора противоречат любому положению Соглашения (включая настоящее ПОД), Стандартные пункты договора имеют преимущественную силу в пределах такого конфликта. Для этого раздела Стандартные договорные положения из Исполнительного решения Комиссии (ЕС) 2021/914 включены посредством ссылки и доступны здесь: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

9.1.2. В отношении Персональных данных, на которые распространяется действие Законов Великобритании о защите данных, применяется Международное соглашение о передаче данных («IDTA») со следующими изменениями: (i) контактная информация о сторонах Соглашения является контактной информацией для IDTA; (ii) Контроллер является экспортером данных, а Обработчик — импортером данных; (iii) законы, регулирующие IDTA, и место, где могут быть поданы судебные иски, — это Англия и Уэльс; (iv) GDPR

Великобритании не применяется к обработке переданных данных импортером; (v) Стороны не используют дополнительные положения о безопасности или коммерческих положениях IDTA; и (vi) информацию в этом ПДО и Приложении 1 можно использовать для Таблиц 1-4. Для этого раздела Стандартные договорные положения Управления Комиссара по информации включены посредством ссылки и доступны здесь: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

9.1.3. В отношении Персональных данных, на которые распространяется действие Швейцарского ПДО, применяются Стандартные договорные положения, указанные в Разделе 9.1.1, со следующими изменениями (i) ссылки на «Регламент (ЕС) 2016/679» должны интерпретироваться как ссылки на швейцарский ПДО; (ii) ссылки на «ЕС», «Союз» и «законодательство государства-члена» должны толковаться как ссылки на швейцарское законодательство; и (iii) ссылки на «компетентный надзорный орган» и «компетентные суды» должны быть заменены на «Федеральный комиссар Швейцарии по защите данных и информации» и «соответствующие суды в Швейцарии».

9.2. Альтернативные механизмы передачи данных. Стороны признают, что законы, правила и положения, касающиеся международной передачи данных, быстро развиваются. В случае, если Контролер использует другой механизм, разрешенный применимыми законами, правилами или положениями для передачи Персональных данных (каждый из которых именуется «Альтернативный механизм передачи данных»), Стороны соглашаются добросовестно работать вместе для реализации любых поправок к настоящему Соглашению, необходимых для реализации Альтернативного механизма передачи данных.

10. ПРОЧИЕ ПОЛОЖЕНИЯ

10.1. Поправки. Настоящий ПОД не может быть изменен или дополнен, и ни одно из его положений не может считаться отмененным или иным образом измененным, кроме как в письменной форме, должным образом оформленной уполномоченными представителями обеих сторон.

10.2 Применимое право. Настоящий ПОД регулируется применимым законодательством, изложенным в Соглашении.

В ПОДТВЕРЖДЕНИЕ ВЫШЕИЗЛОЖЕННОГО стороны данного Соглашения подписали настоящее Соглашение с даты вступления в силу.

КОНТРОЛЛЕР:	**IVANTI**
Подпись: _____	Подпись: _____
Имя: _____	Имя: _____
Должность: _____	Должность: _____
Дата: _____	Дата: _____

Список приложений:

Приложение 1: Описание обработки

ПРИЛОЖЕНИЕ 1

Описание обработки

Контактные данные компании Ivanti:

Ivanti

10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095

Контактные данные должностного лица по защите данных: privacy@ivanti.com

Предмет
Предмет Обработки:
Предоставление лицензий на ИТ-программное обеспечение, услуги поддержки и внедрение, будь то локальное или размещенное решение SaaS, в отношении администрирования и упрощения основных бизнес-процессов в области (областях) унифицированного управления конечными точками, управления ИТ-услугами, управления ИТ-активами, безопасности, отчетности и аналитики, а также цепочки поставок.

ИТ-услуги включают использование программного обеспечения в виде локальной установки или решения SaaS, включая установку модулей (включая, помимо прочего, модули управления неисправностями, изменениями, активами, конфигурацией и выпусками); каталоги самообслуживания и услуг; поддержка и обслуживание, включая, помимо прочего, удаленный доступ; исправления, управление приложениями, безопасность конечных точек/мобильных устройств и управление привилегиями.

Частота Обработки:
Непрерывная.

Продолжительность
Продолжительность Обработки:
Как указано в Соглашении.

Объем, тип и цель Обработки
Объем, тип и цель Обработки следующие:
Как указано в Соглашении.

Субъекты данных
Обработка Персональных данных может относиться к следующим категориям Субъектов данных:
Клиенты, перспективные клиенты; сотрудники; поставщики; торговые представители; контактные лица; подрядчики (включая временных работников); волонтер; временные и эпизодические работники; фрилансеры, агенты, консультанты и другие профессиональные респонденты, а также их соответствующие иждивенцы, бенефициары и контактные лица при чрезвычайных ситуациях; перспективные сотрудники и временный персонал заказчиков; лица, подающие претензию, корреспонденты и лица, выполняющие запрос; советники, консультанты и другие профессиональные эксперты; сотрудники или контактные лица потенциальных клиентов, клиентов, деловых партнеров и поставщиков экспортера данных; деловые партнеры и поставщики экспортера данных (физические лица); и пользователи экспортера данных, уполномоченные экспортером данных на использование программного обеспечения и сопутствующих услуг.

Категории данных
Обрабатываемые персональные данные могут относиться к следующим категориям данных:
Данные Клиента, загружаемые в Службы в рамках служб и учетных записей Клиента.

Организационно-технические мероприятия
Ниже описаны организационно-технические мероприятия по безопасности, реализованные Обработчиком:

Обучение мерам и правилам безопасности
Обработчик проходит обучение по вопросам безопасности, которое включает обязательное обучение по вопросам безопасности при обработке и защите конфиденциальной и частной информации, такой как информация, позволяющая установить личность, информация о финансовом счете и информация о состоянии здоровья, в соответствии с применимым законодательством, а также периодические информационные сообщения и курсы по безопасности, ориентированные на осведомленность конечных пользователей.

Политики и процедуры в сфере безопасности
Обработчик имеет политики информационной безопасности, использования и управления, которые определяют действия сотрудников и подрядчиков в отношении надлежащего использования, доступа и хранения конфиденциальной и частной информации; ограничивают доступ к конфиденциальной и частной информации сотрудникам Обработчика, которым «необходимо знать» такую информацию; предотвращают доступ уволенных сотрудников к информации Обработчика после увольнения; и применяют дисциплинарные меры за несоблюдение такой политики. Системный доступ к ресурсам Обработчика запрещен, если только не проведена специальная оценка и не предоставлен доступ. Обработчик проводит проверку биографических данных своих сотрудников при приеме на работу в установленных законом пределах.

Физический контроль доступа и контроль доступа окружающей среды
Обработчик ограничивает физический доступ к своим информационным системам и объектам с помощью средств физического контроля (например, доступа с кодовым пропуском), которые обеспечивают достаточную уверенность в том, что доступ к его центрам обработки данных разрешен только уполномоченным лицам, и использует камеры или системы видеонаблюдения в критически важных внутренних и внешних точках входа. Обработчик применяет контроль температуры и влажности воздуха в своих центрах обработки данных и защищает от потерь из-за сбоя питания.

Логический контроль доступа
Обработчик использует технологию регистрации и мониторинга для обнаружения и предотвращения попыток несанкционированного доступа к своим сетям и производственным системам. Мониторинг Обработчика включает обзор изменений, влияющих на аутентификацию, авторизацию и аудит систем; привилегированный доступ к производственным системам Обработчика.

Контроль шифрования
Обработчик применяет соответствующие средства контроля шифрованием в своих продуктах. Обработчик оценивает и применяет шифрование при передаче и хранении, используя передовые отраслевые методы для шифрования. Для управления жизненным циклом ключей шифрования, включая генерацию, хранение, управление доступом и ротацию, используются передовые методы.

Контроль уязвимостей
Обработчик регулярно выполняет сканирование уязвимостей и устраняет обнаруженные уязвимости в соответствии с их риском. Продукты Обработчика также подлежат периодической оценке уязвимости и тестированию на проникновение.

Аварийное восстановление и резервное копирование
Обработчик выполняет периодическое резервное копирование производственных файловых систем и баз данных в соответствии с установленным графиком и поддерживает формальный план аварийного восстановления для производственного облачного центра обработки данных, включая регулярное тестирование.

План реагирования на кибер-инциденты
Обработчик применяет план реагирования на инциденты для управления и сведения к минимуму последствий незапланированных киберсобытий, который включает процедуры, которым необходимо следовать в случае фактического или потенциального нарушения безопасности, в том числе: внутренняя группа реагирования на инциденты с руководителем по реагированию; группа по расследованию, проводящая анализ основных

причин и идентифицирующая затронутые стороны; процессы внутренней отчетности и уведомления; документирование ответных действий и планов исправления; и обзор событий после инцидента.

Безопасность хранения и передачи
Обработчик применяет технические меры безопасности для защиты от несанкционированного доступа к данным Обработчика, которые передаются по общедоступной сети электронных коммуникаций или хранятся в электронном виде.

Безопасная утилизация
Обработчик применяет политики и процедуры в отношении утилизации материального и нематериального имущества, содержащего данные Обработчика, таким образом, чтобы данные Обработчика невозможно было прочитать или восстановить на практике.

Идентификация и оценка рисков
Обработчик использует программу оценки рисков, чтобы помочь обоснованно определить предсказуемые внутренние и внешние риски для информационных ресурсов Обработчика и определить, адекватны ли существующие средства контроля, политики и процедуры для устранения выявленных рисков.

Разработчики и поставщики услуг
Сторонние поставщики услуг или разработчики (совместно именуемые «Поставщики»), имеющие доступ к конфиденциальной информации Обработчика, подлежат оценке рисков для определения конфиденциальности передаваемой информации Обработчика. Ожидается, что поставщики будут соблюдать все соответствующие условия контракта, касающиеся безопасности данных Обработчика, а также любые применимые политики или процедуры Обработчика. Периодически Обработчик может просить Поставщика повторно провести оценку его состояние безопасности, чтобы обеспечить соответствие требованиям.