

СОГЛАШЕНИЕ ОБ ОБРАБОТКЕ ДАННЫХ С КОМПАНИЕЙ PIX4D

Последнее изменение: в октябре 2021 г.

Настоящее Соглашение об обработке данных и Приложения к нему (далее совместно — **СОД**) представляет собой соглашение между Вами и компанией Pix4D (далее компания Pix4D и Вы по отдельности именуется **Стороной**, а совместно — **Сторонами**), регулирующее обработку Персональных данных клиентов компанией Pix4D от Вашего имени в связи с Лицензионным соглашением с конечным пользователем (далее — **ЛСКП**). Это СОД является неотъемлемой частью ЛСКП.

Компания Pix4D может периодически пересматривать это СОД. Версия, опубликованная на нашем Веб-сайте pix4d.com/legal, является текущей.

Все термины, употребляемые в этом СОД с заглавной буквы, но специально не определенные в нем, имеют значения, закрепленные за ними в ЛСКП. Во избежание двусмысленного толкования любое упоминание об ЛСКП также означает это СОД (включая его Приложения и СДУ ЕС, как этот термин определен далее) и в максимально допустимом объеме Общие условия компании Pix4D для клиентов (далее — **Общие условия**) и любые дополнительные положения к ним, которые могут применяться в связи с Использованием конкретного Предложения (далее — **Дополнительные условия**).

СОДЕРЖАНИЕ

ПОСКОЛЬКУ.....	3
1. ВСТУПЛЕНИЕ В СИЛУ И СРОК ДЕЙСТВИЯ.....	3
2. СФЕРА ДЕЙСТВИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ДАННЫХ.....	3
3. ОБРАБОТКА ДАННЫХ И ФУНКЦИИ СТОРОН.....	3
4. ЗАПРОСЫ ОТ СУБЪЕКТОВ ДАННЫХ.....	5
5. ПЕРСОНАЛ КОМПАНИИ PIX4D.....	6
6. СУБОБРАБОТЧИКИ.....	6
7. БЕЗОПАСНОСТЬ ДАННЫХ.....	6
8. ПЕРЕДАЧА ДАННЫХ В СТРАНЫ, НЕ ИМЕЮЩИЕ АККРЕДИТАЦИИ.....	7
9. НАРУШЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ.....	8
10. ТРЕБОВАНИЯ ДОСТУПА К ДАННЫМ СО СТОРОНЫ ГОСУДАРСТВА.....	9
11. ПРОВЕРКА И ОЦЕНКА СОБЛЮДЕНИЯ ОБЯЗАТЕЛЬСТВ.....	9
12. ОЦЕНКИ ПОСЛЕДСТВИЙ И КОНСУЛЬТАЦИИ.....	9
13. ВОЗВРАТ ИЛИ УДАЛЕНИЕ ДАННЫХ.....	9
14. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ.....	10
15. ПРОЧИЕ ПОЛОЖЕНИЯ.....	10
16. ПРИМЕНИМОЕ ЗАКОНОДАТЕЛЬСТВО — УРЕГУЛИРОВАНИЕ СПОРОВ.....	11

17.	ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ О ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ШТАТА КАЛИФОРНИЯ.....	11
18.	ОПРЕДЕЛЕНИЯ.....	11

ПОСКОЛЬКУ

- А. Стороны заключили ЛСКП в соответствии с Общими условиями и Дополнительными условиями, в зависимости от обстоятельств.
- В. В целях исполнения ЛСКП компания Pix4D и/или любые ее Аффилированные лица могут иметь доступ к Персональным данным клиента, раскрытым или иным образом предоставленным Вами (или по Вашему указанию) либо Авторизованными пользователями в связи с Лицензированными предложениями в соответствии с ЛСКП.
- С. Поскольку компания Pix4D будет обрабатывать такие Персональные данные клиентов как Ваш обработчик, Стороны намерены обеспечить соответствие такой обработки применимым Законам о защите персональных данных и согласовать некоторые условия такой обработки в соответствии с этим СОД.

Таким образом, Стороны заключили настоящее соглашение о нижеследующем:

1. ВСТУПЛЕНИЕ В СИЛУ И СРОК ДЕЙСТВИЯ

- 1.1. **Вступление в силу.** Это СОД вступает в силу с Даты вступления в силу Условий (как определено ниже) и заменяет собой любое применимое предыдущее соглашение об обработке данных.
- 1.2. **Срок действия.** Независимо от истечения срока действия или расторжения ЛСКП, настоящее СОД (включая положения об О — К, если применимо) автоматически прекращает свое действие только после того, как компания Pix4D удалит все Данные клиента в соответствии с условиями этого СОД.

2. СФЕРА ДЕЙСТВИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ДАННЫХ

- 2.1. **Применение законов о защите персональных данных.** Стороны подтверждают, что на обработку Персональных данных клиентов компанией Pix4D распространяется Законодательство ЕС о защите данных, а также, в зависимости от обстоятельств, Неевропейское законодательство о защите данных.
- 2.2. **Применение положений этого СОД.** Настоящее СОД составлено специально для целей Законодательства ЕС о защите данных, но также в нем по мере возможности учтены применимые требования Неевропейского законодательства о защите данных, в частности Закона Калифорнии о защите персональных данных потребителей (CCPA), изложенные в разделе 17.. При отсутствии в этом СОД положений об обратном настоящее СОД действует независимо от применения Законодательства ЕС о защите данных или Неевропейского законодательства о защите данных к обработке Персональных данных клиентов.

3. ОБРАБОТКА ДАННЫХ И ФУНКЦИИ СТОРОН

- 3.1. **Функции Сторон** В тех случаях, когда применяется Законодательство ЕС о защите данных, Стороны признают и соглашаются с тем, что в части обработки Персональных данных клиентов при исполнении ЛСКП в отношении: (i) Авторизованных пользователей Лицензированных предложений, Учетными записями которых Вы управляете (и, в частности, определяете, кто и в какой степени имеет доступ к Организации); и/или (ii) любого другого третьего лица, фигурирующего в Контенте, раскрытие или иное предоставление которого компании Pix4D происходит в связи с Лицензированными предложениями в соответствии с ЛСКП, Вы являетесь

контролером, а компания Pix4D — обработчиком, действующим от Вашего имени.

3.2. **Дальнейшая обработка компанией Pix4D.** Невзирая на положения вышеприведенного раздела 3.1., Вы соглашаетесь с тем, что компания Pix4D может обрабатывать Персональные данные не только в роли обработчика, но и в роли контролера для своих собственных целей в указанных ниже случаях.

- (a) В отношении Персональных данных Авторизованных пользователей Лицензированных предложений, включая данные об использовании, если это необходимо для работы Лицензированных приложений (например, для создания счетов-фактур) и другого выполнения ЛСКП либо осуществления собственных прав; в частности, для данных об использовании, если (a) такое использование служит для статистических, аналитических и других целей, не связанных с определенными физическими лицами, и (b) любую информацию, если таковая имеется, к которой предоставлен доступ третьим лицам (отличным от поставщиков услуг Pix4D, обязавшихся соблюдать конфиденциальность), которая (i) не содержит персональных данных, по которым можно идентифицировать Авторизованных пользователей, и (ii) не содержит персональных данных, по которым можно идентифицировать Вас; при этом пункты (a) и (b) не применяются, мы будем обрабатывать неанонимизированные данные об использовании в целях аналитики использования и улучшения продукта, только если Вы согласились на такую обработку в своих настройках конфиденциальности персональной Учетной записи.
- (b) В отношении Персональных данных третьих лиц в Контенте, который раскрыт или иным образом стал доступным компании Pix4D через Лицензированное предложение, для своих собственных целей в роли контролера, если (a) такое использование служит для целей статистики, исследований и разработки, сравнительного анализа и пр., не связанных с определенными физическими лицами, и (b) любую информацию, если таковая имеется, к которой предоставлен доступ третьим лицам (отличным от поставщиков услуг Pix4D, обязавшихся соблюдать конфиденциальность), которая (i) не содержит персональных данных, по которым можно идентифицировать третьих лиц, и (ii) не содержит персональных данных, по которым можно идентифицировать Вас.
- (c) Во всех случаях для любых прочих целей, если это требуется или разрешено Законодательством о защите данных и другими применимыми законами.

3.3. **Соблюдение Вами нормативных требований и Ваши указания для компании Pix4D.** Вы заявляете и гарантируете, что: (i) Вы соблюдаете и будете соблюдать все применимые законы, в т. ч. Законодательство о защите данных, в ходе обработки Вами Персональных данных клиентов, при поручении этой задачи компании Pix4D и при предоставлении Вами ей любых указаний касательно обработки; и (ii) Вы предоставили и будете предоставлять все уведомления, а также получили и будете получать все разрешения и права, которые необходимы компании Pix4D по Законодательству о защите данных для обработки Персональных данных клиентов в целях, описанных в ЛСКП. Вы несете исключительную ответственность за достоверность, качество, законность и способы получения Вами Персональных данных клиентов. Без ограничения общего смысла вышеизложенного Вы соглашаетесь с тем, что Вы несете

ответственность за соблюдение всех законов (включая Законодательство о защите данных), которые распространяются на любой Контент, создаваемый, передаваемый или управляемый посредством Лицензированных предложений в соответствии с ЛСКП. Настоящим Вы предоставляете компании Pix4D разрешение и указание самостоятельно осуществлять управление и обработку запросов на удаление Учетной записи пользователя от Вашего имени, если (i) такие запросы отправлены Пользователем непосредственно в компанию Pix4D на адрес data_protection@pix4d.com другими способами и (ii) Пользователь является одним из Ваших Авторизованных пользователей. В таком случае компания Pix4D может уведомить Вас о таком запросе на удаление учетной записи, если сочтет необходимым. ЛСКП (включая настоящее СОД), а также Использование и способ, посредством которого Вы осуществили настройку Лицензированных продуктов в соответствии с ЛСКП, представляют собой все Ваши указания для компании Pix4D в отношении обработки Персональных данных клиентов, при этом в течение Срока действия Вы можете предоставлять дополнительные указания, соответствующие требованиям ЛСКП, характеру, сфере применения и утвержденному использованию Лицензированных продуктов, и при отсутствии иных условий несете ответственность за любые связанные с этим расходы. Компания Pix4D незамедлительно уведомит Вас в письменной форме, если ей станет известно или она решит, что какие-либо Ваши указания касательно обработки данных нарушают Законодательство ЕС о защите данных.

- 3.4. **Обязательства компании Pix4D.** Компания Pix4D обрабатывает Персональные данные клиентов в соответствии с ЛСКП, применимым Законодательством о защите данных и Вашими документально оформленными правомерными указаниями на условиях, изложенных в разделе 3.2..
- 3.5. **Обработка.** Предметом обработки Персональных данных клиентов компанией Pix4D является исполнение ЛСКП. Типы персональных данных и категории субъектов данных, периодичность и цель передачи, характер обработки, срок хранения данных и детали их субобработки более подробно изложены в Приложении С (Описание передачи данных) к этому СОД.

4. ЗАПРОСЫ ОТ СУБЪЕКТОВ ДАННЫХ

Если в течение Срока действия компания Pix4D получит от какого-либо субъекта данных запрос на осуществление им своих прав как субъекта данных в соответствии с Законодательством ЕС о защите данных в отношении Персональных данных клиента, в таком случае компания Pix4D: (i) порекомендует субъекту данных направить свой запрос Вам; (ii) незамедлительно уведомит Вас об этом; и (iii) без Вашего предварительного разрешения никаким другим образом не будет напрямую реагировать на запрос такого субъекта данных, а будет действовать исходя из ситуации (например, сообщит субъекту данных, чтобы он обратился к Вам) или в соответствии с законом. Кроме того, принимая во внимание характер обработки, компания Pix4D обязуется оказывать Вам посильную дополнительную помощь в исполнении Вами своих обязательств по защите данных в отношении прав субъектов данных, предусмотренных Законодательством ЕС о защите данных. На основании предварительной письменной договоренности между Сторонами Вы соглашаетесь возместить компании Pix4D все издержки и расходы, обоснованно понесенные ею при оказании Вам помощи в соответствии с положениями этого раздела 4..

5. ПЕРСОНАЛ КОМПАНИИ PIX4D

Компания Pix4D гарантирует, что все лица, уполномоченные ею обрабатывать Персональные данные клиентов (в т. ч. ее персонал, агенты и субподрядчики), несут надлежащую ответственность по соблюдению конфиденциальности (по договору или закону), в частности они обязались не разглашать Персональные данные клиентов третьим лицам, а также обрабатывать такие данные исключительно для выполнения задач, возложенных на них компанией Pix4D в соответствии с ЛСКП. Стороны также договорились о том, что компания Pix4D несет ответственность за действия любого своего персонала как за собственные действия.

6. СУБОБРАБОТЧИКИ

- 6.1. **Уполномоченные субобработчики.** Вы соглашаетесь с тем, что компания Pix4D может привлекать субобработчиков для обработки Персональных данных клиентов от Вашего имени. Субобработчики, в настоящее время задействованные компанией Pix4D и уполномоченные Вами, являются: (i) Аффилированными лицами компании Pix4D; и (ii) третьими лицами, включенными в список субобработчиков Pix4D, с которым можно ознакомиться по адресу <https://www.pix4d.com/legal>. Кроме того, настоящим Вы предоставляете компании Pix4D общее письменное разрешение назначить любого другого субобработчика в соответствии с этим разделом 6. для выполнения определенных действий по обработке от имени компании Pix4D.
- 6.2. **Право на возражение против изменений субобработчиков.** В случаях, предусмотренных Законодательством ЕС о защите данных, компания Pix4D обязуется уведомлять Вас обо всех планируемых изменениях, которые предполагают назначение новых или смену существующих субобработчиков, при этом Вы вправе обоснованно возразить против таких изменений в течение 30 (тридцати) дней после получения уведомления. Если Вы возразите против изменений в установленный выше срок, у Вас будет возможность обсудить свои возражения с компанией Pix4D и достичь с ней приемлемой с экономической точки зрения договоренности. Если такой договоренности достичь не удастся, компания Pix4D либо откажется от назначения нового субобработчика, либо позволит Вам расторгнуть ЛСКП в соответствии с его положениями о прекращении его действия без штрафных санкций (при этом Вы будете должны совершить все платежи, обязательства по которым возникли у Вас до прекращения действия ЛСКП).
- 6.3. **Ответственность в связи с назначением субобработчика.** Назначая любого субобработчика, компания Pix4D гарантирует, что он будет нести как минимум такую же строгую ответственность по обеспечению конфиденциальности и защите персональных данных, как та, что предусмотрена ЛСКП (включая это СОД), в объеме, применимом к характеру обработки, выполняемой таким субобработчиком. Кроме того, Стороны также договорились о том, что компания Pix4D несет ответственность как за действия всех своих субобработчиков, так и за собственные действия.

7. БЕЗОПАСНОСТЬ ДАННЫХ

Компания Pix4D обязуется внедрять и поддерживать соответствующие организационно-технические меры по защите Персональных данных клиентов от случайного или незаконного уничтожения, потери, изменения, несанкционированного раскрытия или доступа, в частности как минимум меры, изложенные в Приложении D (Меры безопасности) к этому СОД

(далее — **Меры безопасности**). К Мерам безопасности относятся меры по шифрованию Персональных данных клиента для постоянного обеспечения конфиденциальности, целостности, доступности и отказоустойчивости систем и сервисов компании Pix4D, оперативного восстановления доступа к Персональным данным клиентов после Нарушения безопасности данных, а также для регулярного тестирования эффективности. Вы обязаны ознакомиться с предоставленной Вам компанией Pix4D информацией о безопасности данных и самостоятельно решить, соответствуют ли Меры безопасности Вашим требованиям и правовым обязательствам по Законодательству о защите данных. Вы понимаете, что Меры безопасности зависят от прогресса и достижений в области науки и техники и что компания Pix4D может периодически обновлять или изменять Меры безопасности при условии, что это не приведет к ослаблению общей безопасности предоставляемых Вам Лицензированных предложений.

8. ПЕРЕДАЧА ДАННЫХ В СТРАНЫ, НЕ ИМЕЮЩИЕ АККРЕДИТАЦИИ

8.1. **СДУ ЕС.** Стороны договариваются о том, что для целей ЛСКП или в связи с его исполнением компания Pix4D может передавать Персональные данные клиентов в страны, не имеющие Аккредитации. В случае передачи компанией Pix4D Персональных данных клиентов в соответствии с Законодательством ЕС о защите данных (обратно) Вам как контролеру, находящемуся в стране, не имеющей Аккредитации, Стороны обязуются соблюдать требования Модуля 4 (Передача данных обработчиком контролеру) Стандартных договорных условий ЕС, изложенные в Приложении А (Модуль 4 (Передача данных обработчиком контролеру) СДУ ЕС) в указанном ниже составе (далее — **Положения об О — К**), в т. ч. любые применимые поправки для конкретной страны, указанные в Приложении В (далее — Поправки к СДУ ЕС для конкретной страны) к этому СОД, при этом компания Pix4D является экспортером данных, а Вы — импортером данных:

- (d) пп. 1—6;
- (e) п. 7 не применяется;
- (f) п. 8 с положениями для «Модуля 4», включая вступительный абзац;
- (g) п. 10 с положениями для «Модуля 4»;
- (h) п. 11(a), исключая положения «Вариант» п. 11(a);
- (i) п. 12 с положениями для «Модуля 4»; в случаях, предусмотренных СДУ ЕС, ответственность между импортером данных и экспортером данных (но не перед субъектами данных) ограничивается/исключается в соответствии с разделом 14 настоящего СОД;
- (j) пп. 14—15 с положениями для «Модуля 4», если экспортер данных объединяет персональные данные, полученные от импортера данных, с персональными данными, собранными экспортером данных в стране, имеющей Аккредитацию;
- (k) п. 16 с положениями для «Модуля 4»;
- (l) п. 17 с положениями для «Модуля 4», при этом Стороны соглашаются подчиняться законодательству Франции в случаях, установленных в п. 17;
- (m) п. 18 с положениями для «Модуля 4», при этом Стороны соглашаются подчиняться юрисдикции судов Франции в случаях, установленных в п. 18.

8.2. **Приложения к СДУ ЕС.** Приложения, указанные в Положениях об О — К, формулируются следующим образом:

(а) Приложение I.A должно содержать:

- i. информацию, указанную в ЛСКП и предоставленную Вами в соответствующей Форме организации, при этом компания Pix4D является экспортером данных, действующим в качестве обработчика, а Вы — импортером данных, действующим в качестве контролера;
- ii. контактные данные экспортера данных. Контактные данные экспортера данных: Pix4D SA, Route de Renens 24, 1008 Prilly, Switzerland (Швейцария). С отделом защиты данных экспортера данных можно связаться по адресу электронной почты: data_protection@pix4d.com. Контактная информация директора по защите данных экспортера данных: Parrot Drones, Виктор Вюяр (Victor Vuillard), 174 Quai de Jemmapes, 75010 Paris, France (Франция);
- iii. контактная информация импортера данных. Контактная информация импортера данных, включая контактные данные его директора по защите данных, указаны для экспортера данных в соответствующей Форме организации (если такие сведения были предоставлены импортером данных) и/или доступны экспортеру данных по запросу в любое время;
- iv. действия, указанные в Приложении С (Описание передачи) к настоящему СОД;
- v. Стороны соглашаются, что исполнение ЛСКП импортером данных и экспортером данных означает выполнение этих Положений об О — К обеими Сторонами с Даты вступления Условий в силу.

(b) Приложение I.B должно содержать соответствующий раздел Приложение С (Описание передачи);

(c) Приложение II должно состоять из Приложения В (Организационно-технические меры) к настоящему СОД.

(d) В соответствующих случаях Приложение III должно содержать список субобработчиков компании Pix4D, размещаемый по адресу <https://www.pix4d.com/legal>.

8.3. **Оценка последствий передачи данных.** Заказчик признаёт, что, насколько ему известно, планируемые передачи персональных данных от компании Pix4D (обратно) Заказчику не противоречат действующему законодательству, и у Сторон нет оснований полагать, что такие передачи данных являются несанкционированными.

8.4. **Гарантия защиты от убытков.** Стороны обязуются возместить друг другу ущерб в случае предъявления третьими лицами претензий в связи с нарушением Сторонами обязательств, предусмотренных Условиями передачи О — К.

9. НАРУШЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ

Как только компании Pix4D станет известно о Нарушении безопасности данных, она обязуется: (i) уведомить Вас без ненужных проволочек, по возможности в течение 48 (сорока восьми) часов с момента обнаружения Нарушения безопасности данных; (ii) предоставить актуальную

информацию о Нарушении безопасности данных, как только она станет известной или по Вашему обоснованному запросу; и (iii) незамедлительно принять соответствующие меры для минимизации последствий, а также для расследования любого Нарушения безопасности данных. Предоставление компанией Pix4D уведомления или ответа на Нарушение безопасности данных в соответствии с настоящим разделом 9. не означает признание компанией Pix4D вины или ответственности в связи с Нарушением безопасности данных.

10. ТРЕБОВАНИЯ ДОСТУПА К ДАННЫМ СО СТОРОНЫ ГОСУДАРСТВА

Осуществляя обработку Персональных данных клиентов как Ваш обработчик в соответствии с Законодательством ЕС о защите персональных данных, компания Pix4D не предоставляет органам государственной власти, в т. ч. правоохранительным, доступ или информацию об Учетных записях Pix4D, включая Данные клиентов, за исключением случаев, предусмотренных действующим законодательством. Вы несете расходы, связанные с предоставлением ответа на обязательный запрос (будь то в форме повестки в суд, постановления суда, ордера на обыск или другого надлежащего судебного приказа) любого органа государственной власти, в т. ч. правоохранительного, на доступ к Учетной записи Pix4D или информации о ней, включая Данные клиентов, принадлежащие Вам и/или Авторизованным пользователям.

11. ПРОВЕРКА И ОЦЕНКА СОБЛЮДЕНИЯ ОБЯЗАТЕЛЬСТВ

Компания Pix4D обязуется предоставить Вам всю необходимую информацию, подтверждающую соблюдение Pix4D своих обязательств по настоящему СОД, а также разрешит Вам или назначенному Вами независимому аудитору проводить проверки, включая инспекции, соблюдения компанией Pix4D своих обязательств по настоящему СОД, и будет содействовать в проведении таких проверок, при условии соблюдения стандартных требований обеспечения конфиденциальности. Кроме того, компания Pix4D может бесплатно, по собственной инициативе или в ответ на запрос предоставить Вам любой составленный аудитором компании Pix4D отчет о проведении проверки соблюдения компанией Pix4D требований этого СОД.

12. ОЦЕНКИ ПОСЛЕДСТВИЙ И КОНСУЛЬТАЦИИ

В случаях, предусмотренных действующим Законодательством о защите данных, компания Pix4D обязуется предоставить Вам в ответ на Ваш надлежащим образом оформленный запрос, с учетом характера обработки и имеющейся у компании Pix4D информации, сведения о Лицензированных предложениях, чтобы Вы могли оценить последствия для безопасности данных или провести предварительные консультации с органами по защите данных в соответствии с требованиями Законодательства о защите данных. На основании предварительной письменной договоренности между Сторонами Вы обязуетесь возместить компании Pix4D все издержки и расходы, обоснованно понесенные ею при оказании Вам помощи в соответствии с положениями этого раздела 12..

13. ВОЗВРАТ ИЛИ УДАЛЕНИЕ ДАННЫХ

После расторжения или истечения срока действия ЛСКП компания Pix4D (на Ваш выбор) удалит (в частности, путем анонимизации) или вернет Вам все Персональные данные клиентов (включая их копии), которые находятся

в ее распоряжении или под ее контролем; данное требование не применяется в случае, если компания Pix4D должна в соответствии с применимым законодательством хранить некоторые или все Персональные данные клиентов, а также оно не применяется к Персональным данным клиентов, заархивированным в системах резервного копирования, которые компания Pix4D обязана надежно изолировать, сделать недоступными для дальнейшей обработки и со временем удалить в соответствии со своей политикой удаления данных, за исключением случаев, предусмотренных применимым законодательством.

14. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

За исключением случаев, предусмотренных Условиями передачи О — К в разделах 8.1. и 8.2., и кроме случаев, прямо оговоренных в этом СОД, ответственность компании Pix4D и Ваша ответственность ограничиваются настолько, насколько позволяет применимое законодательство.

15. ПРОЧИЕ ПОЛОЖЕНИЯ

15.1. **Поправки.** Все поправки к настоящему СОД оформляются в письменном виде и подписываются уполномоченными представителями Сторон.

15.2. **Противоречия.** В случае возникновения противоречий или несоответствий между настоящим СОД и ЛСКП касательно обработки Персональных данных клиентов преимущественную силу имеют положения следующих документов (в порядке приоритетности): (i) СДУ ЕС; (ii) это СОД; (iii) ЛСКП.

15.3. **Независимость положений Соглашения.** Если какое-либо положение СОД будет по какой-либо причине признано не имеющим исковой силы, по возможности оно должно быть не аннулировано, а исправлено с максимальным учетом изначальных правовых и экономических намерений Сторон. В любом случае все остальные положения этого СОД остаются в силе и подлежат исполнению в максимально возможном объеме.

15.4. **Уведомления.** В целях письменного обмена информацией между Сторонами все уведомления или иные сообщения, связанные с ЛСКП, должны оформляться письменно (электронный формат допускается) и отправляться по электронной почте на указанные ниже адреса:

Для компании Pix4D: адрес электронной почты: legal@pix4d.com.

Для Вас: адрес электронной почты, указанный в Вашей Учетной записи. Вы обязаны уведомлять компанию Pix4D обо всех изменениях Ваших контактных данных. Для этого Вы можете обратиться в отдел поддержки клиентов компании Pix4D по адресу <https://support.pix4d.com> или обновить свои контактные данные в своей Учетной записи.

Система электронной связи компании Pix4D (в случае ее использования) служит единственным средством подтверждения содержания, времени доставки и получения упомянутых выше электронных сообщений.

15.5. **Расходы.** Стороны несут ответственность за свои расходы, связанные с соблюдением этого СОД, включая Условия передачи О — К в соответствующих случаях.

16. ПРИМЕНИМОЕ ЗАКОНОДАТЕЛЬСТВО — УРЕГУЛИРОВАНИЕ СПОРОВ

16.1. **Применимое законодательство.** Независимо от применимого законодательства ЛСКП, настоящее СОД регулируется и истолковывается исключительно в соответствии с нормами материального права Швейцарии, и к нему не применяются: (i) международные конвенции, в т. ч. Конвенция Организации Объединенных Наций о договорах международной купли-продажи товаров от 11.04.1980 (КМКПТ); и (ii) нормы коллизионного права Швейцарии.

16.2. **Юрисдикция и место урегулирования споров.** Независимо от юрисдикции ЛСКП, любые споры, которые могут возникнуть между Сторонами в результате этого СОД или в связи с ним, рассматриваются только обыкновенными судами Лозанны, Швейцария.

17. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ О ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ШТАТА КАЛИФОРНИЯ

17.1. **Сфера действия и применимость.** Этот раздел 17. СОД применяется в дополнение к его условиям, если компания Pix4D обрабатывает Персональную информацию жителей штата Калифорния в соответствии с ЛСКП согласно Закону Калифорнии о защите персональных данных потребителей (ССРА). В случае возникновения каких-либо расхождений или неоднозначности между этим разделом 17. и любыми другими условиями настоящего СОД, этот раздел 17. имеет преимущественную силу, но лишь в том объеме, в каком он применяется к компании Pix4D.

17.2. **Функции Сторон** Стороны подтверждают и соглашаются с тем, что в процессе обработки Персональной информации жителей штата Калифорния в соответствии с Вашими указаниями Вы являетесь Бизнесом, а компания Pix4D — Поставщиком услуг, как эти термины определены в ССРА.

17.3. **Обязанности.** Стороны соглашаются с тем, что компания Pix4D будет обрабатывать Персональную информацию жителей штата Калифорния как Поставщик услуг исключительно с целью выдачи лицензий на Лицензированные предложения в соответствии с ЛСКП (далее — **Деловая цель**) или в иных целях, не противоречащих ССРА.

18. ОПРЕДЕЛЕНИЯ

Дополнительные условия	этот термин имеет определение, изложенное на первой странице.
-------------------------------	---

Авторизованные пользователи	означает лиц, которым Вы разрешаете использовать Лицензированные продукты в соответствии с ЛСКП. Уточнение: авторизованными пользователями могут быть Ваши сотрудники, аффилированные лица и другие третьи лица, не входящие в состав Вашего предприятия, надлежащим образом уполномоченные администратором Вашей учетной записи на вступление в Организацию, в которой Вы выполняете функцию контролера этих третьих лиц.
------------------------------------	--

Бизнес	этот термин имеет значение, закрепленное за ним в
---------------	---

ССРА.

Деловая цель	этот термин имеет значение, закрепленное за ним в разделе 17.3..
Персональная информация жителей штата Калифорния ССРА	означает Персональные данные, подпадающие под защиту согласно ССРА. означает раздел 1798.100 и след. Гражданского кодекса штата Калифорния, иначе именуемый Законом Калифорнии о защите персональных данных потребителей 2018 г.
CNIL	означает Commission Nationale de l'Informatique et des Libertés (Национальную комиссию по информатике и свободам), как этот термин определен в разделе 8.2..
Потребитель	этот термин имеет значение, закрепленное за ним в ССРА.
Контролер	означает физическое или юридическое лицо, государственный орган, ведомство или другое учреждение, которые самостоятельно или совместно с другими лицами определяют цели и способы обработки персональных данных.
Данные клиентов	означают данные, предоставленные Вами или Конечными пользователями либо от Вашего имени через Лицензированные предложения и под Учетной записью.
Персональные данные клиентов	означают персональные данные, входящие в состав Данных клиента, включая все особые категории персональных данных.
Нарушение безопасности данных	означает нарушение безопасности, ведущее к случайному или неправомерному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к персональным данным, передаваемым, сохраняемым или иным образом обрабатываемым компанией Pix4D, в частности любое нарушение положений <u>Приложения D (Меры безопасности)</u> .
Законодательство о защите данных	о означает все законы и нормативно-правовые акты о защите данных, применимые к обработке компанией Pix4D или Вами Персональных данных клиентов в соответствии с ЛСКП, включая, в зависимости от обстоятельств, Законодательство ЕС о защите данных и Неевропейское законодательство о защите данных.
Субъект данных	означает любое опознанное или опознаваемое физическое лицо, к которому относятся персональные данные.

Запрос от субъекта данных	этот термин имеет значение, закрепленное за ним в разделе 4..
СОД	этот термин имеет определение, изложенное на первой странице.
ЕЭП	означает Европейское экономическое пространство
ЛСКП	этот термин имеет определение, изложенное на первой странице.
СДУ ЕС	означает стандартный договор, утвержденный Решением Европейской комиссии от 4 июня 2021 г. [C(2021)3972, окончательный вариант] о стандартных договорных условиях передачи персональных данных в третьи страны в соответствии с Регламентом (ЕС) № 2016/679 Европейского парламента и Совета, включая все поправки к нему.
Законодательство ЕС о защите данных	означает, в соответствующих случаях: (a) Общий регламент ЕС по защите данных (GDPR) и любое реализующее его местное, региональное или национальное законодательство; (b) GDPR Великобритании; и (c) Закон о защите данных Швейцарии и в каждом отдельном случае любую новую или пересмотренную версию, которая может вступить в силу в течение Срока действия.
FDPIC	означает федерального уполномоченного Швейцарии по защите данных и информации (Swiss Federal Data Protection and Information Commissioner), как этот термин определен в разделе 8.2..
GDPR	означает Регламент (ЕС) № 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных, а также об отмене Директивы № 95/46/ЕС и любую новую или пересмотренную версию этого документа, которая может вступить в силу в течение Срока действия.
Общие условия	этот термин имеет определение, изложенное на первой странице.
Неевропейское законодательство о защите данных	означает законы о защите данных или конфиденциальности, действующие за пределами ЕЭП, Великобритании и Швейцарии, в частности ССРА.
Форма организации	означает параметры Организации в Управлении корпоративными пользователями, предоставленные компанией Pix4D для регистрации Вашей Учетной записи.
Стороны	этот термин имеет определение, изложенное на первой странице.
Условия передачи	означает Модуль 4 (Передача данных обработчиком

О — К	контролеру) СДУ ЕС в составе, указанном в разделах 8.1. и 8.2. настоящего СОД.
Pix4D, Мы, включая словоформы местоимений	Наш, все этих Pix4D SA, швейцарское акционерное общество (<i>société anonyme</i>), зарегистрированное в Швейцарии под номером CHE-207.009.701, юридический адрес: Route de Renens 24, 1008 Prilly, Switzerland (Швейцария).
Меры безопасности	означают организационно-технические меры безопасности, изложенные в <u>Приложении D</u> (<i>Меры безопасности</i>).
Поставщик услуг	этот термин имеет значение, закрепленное за ним в CCPA.
Закон о защите данных Швейцарии	означает Федеральный закон Швейцарии о защите данных от 19 июня 1992 г. и Постановление правительства Швейцарии о Федеральном законе о защите данных от 14 июня 1993 г. и в каждом отдельном случае любую новую или пересмотренную версию этих документов, которая может вступить в силу в течение Срока действия.
Срок действия	означает промежуток времени с Даты вступления Условий в силу до окончания предоставления компанией Pix4D Лицензированных предложений, включая, в соответствующих случаях, период, на который может быть приостановлено предоставление Лицензированных предложений, и период после прекращения действия, в течение которого компания Pix4D может продолжать предоставлять Лицензированные предложения или выполнять переходные задачи.
Дата вступления Условий в силу	означает дату принятия Вами или иного согласования Сторонами этого СОД.
GDPR Великобритании	означает GDPR ЕС с поправками, включенными в законодательство Великобритании в соответствии с Законом Великобритании о выходе из Европейского союза 2018 г., и применимые производные нормативно-правовые акты, принятые в соответствии с этим Законом, любую их новую или пересмотренную версию, которая может вступить в силу в течение Срока действия.
Страны, имеющие Аккредитацию,	означают: - в отношении Персональных данных клиентов, подпадающих под действие GDPR: ЕЭП или любую страну/территорию, по которой Европейская комиссия вынесла решение о достаточности мер в соответствии со ст. 45(1) GDPR; - в отношении Персональных данных клиентов,

- подпадающих под действие GDPR Великобритании: Великобританию или любую страну/территорию, на которую распространяются правила о достаточности мер, предусмотренные ст. 45(1) GDPR Великобритании и разделом 17A Закона о защите данных 2018 г.; и/или*
- *в отношении Персональных данных клиентов, попадающих под действие Закона о защите данных Швейцарии: Швейцарию или любую страну/территорию: (i) включенную в список государств, законодательство которых обеспечивает достаточные меры защиты данных, публикуемый федеральным уполномоченным Швейцарии по защите персональных данных и информации; или, в зависимости от обстоятельств, (ii) попадающую под действие решения Федерального совета Швейцарии о достаточности мер, предусмотренных Законом о защите данных Швейцарии.*

Вы и Ваш, включая все словоформы этих местоимений, означает юридическое лицо, выдающее лицензии на Лицензированные предложения согласно ЛСКП для использования его Авторизованными пользователями.

Термины «персональные данные», «субъект данных», «обработка», «контролер» и «обработчик», используемые в этом СОД, имеют значения, закрепленные за ними в GDPR, независимо от применения Законодательства ЕС о защите данных или Неевропейского законодательства о защите данных.

Дополнения:

Приложение А: Модуль 4 (Передача данных обработчиком контролеру) СДУ ЕС
Приложение В: Поправки к СДУ ЕС для конкретных стран
Приложение С: Описание передачи
Приложение D: Меры безопасности

РАЗДЕЛ I

Условие 1

Цель и сфера применения

- a) Цель этих стандартных договорных условий состоит в том, чтобы обеспечить соблюдение требований Регламента (ЕС) № 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (далее — **Общий регламент по защите данных**)⁽¹⁾ для передачи персональных данных в третью страну.
- (b) Стороны:
- (i) физические или юридические лица, государственные органы, агентства или другие учреждения (далее — **организации**), передающие персональные данные в соответствии с Приложением I.A (в дальнейшем каждая из них по отдельности именуется **экспортером данных**); и
 - (ii) организации в третьей стране, получающие персональные данные от экспортера данных, прямо или опосредованно через другую организацию, также являющуюся Стороной этих Условий, как изложено в Приложении I.A (в дальнейшем каждая из них по отдельности именуется **импортером данных**)
- согласовали эти стандартные договорные условия (далее — **Условия**).
- (c) Эти Условия применяются к передаче персональных данных в соответствии с Приложением I.B.
- (d) Дополнение к этим Условиям, включающее в себя упомянутые в нем Приложения, является неотъемлемой частью этих Условий.

Условие 2

Действие и неизменность Условий

- (a) Эти Условия устанавливают соответствующие гарантии, в т. ч. обеспеченные исковой силой права субъектов данных и эффективные средства правовой защиты, предусмотренные ст. 46(1) и ст. 46(2)(с) Регламента (ЕС) № 2016/679, а в отношении передачи данных от контролеров обработчикам и/или от обработчиков обработчикам — стандартные договорные условия, предусмотренные ст. 28(7) Регламента (ЕС) № 2016/679, без возможности их изменения, кроме выбора соответствующего Модуля или Модулей либо включения информации в Дополнение или ее обновления. При этом Стороны вправе включать стандартные договорные условия, изложенные в этих Условиях, в более

¹ Если экспортер данных является обработчиком, на которого распространяется действие Регламента (ЕС) № 2016/679, действующим от имени учреждения или органа Союза как контролер, применение этих пунктов при привлечении другого обработчика (субобработчика), не подпадающего под действие Регламента (ЕС) № 2016/679, также обеспечивает соблюдение ст. 29(4) Регламента (ЕС) № 2018/1725 Европейского парламента и Совета от 23 октября 2018 г. о защите физических лиц при обработке персональных данных учреждениями, органами, службами и агентствами Союза, и о свободном перемещении таких данных, а также об отмене Регламента (ЕС) № 45/2001 и Постановления № 1247/2002/ЕС (Официальный вестник Европейского союза, вып. L 295, 21.11.2018, стр. 39) в объеме взаимного согласования этих статей и обязательств по защите данных, как изложено в договоре или другом юридически значимом акте между контролером и обработчиком в соответствии со ст. 29(3) Регламента (ЕС) № 2018/1725. В частности, это положение применяется, если контролер и обработчик полагаются на стандартные договорные условия, изложенные в Постановлении № 2021/915.

широкий договор и/или добавлять другие положения или дополнительные гарантии, ни прямо, ни косвенно не противоречащие этим Условиям и не ограничивающие основные права и свободы субъектов данных.

- (b) Эти Условия не ограничивают обязательства экспортера данных в соответствии с Регламентом (ЕС) № 2016/679.

Условие 3

Сторонние бенефициары

- (a) Субъекты данных могут применять и обеспечивать соблюдение настоящих Условий как сторонние бенефициары в отношениях с экспортером данных и/или импортером данных с указанными ниже исключениями:
- (i) Условие 1, Условие 2, Условие 3, Условие 6, Условие 7;
 - (ii) Условие 8.1(b) и Условие 8.3(b);
 - (iii) неприменимо;
 - (iv) неприменимо;
 - (v) Условие 13;
 - (vi) Условие 15.1(c), (d) и (e);
 - (vii) Условие 16(e);
 - (viii) Условие 18.
- (b) Пункт (a) не ограничивает права субъектов данных, предусмотренные Регламентом (ЕС) № 2016/679.

Условие 4

Толкование

- (a) В случае использования в этих Условиях терминов, определенных в Регламенте (ЕС) № 2016/679, эти термины имеют то же значение, что и в Регламенте.
- (b) Эти Условия истолковываются в контексте положений Регламента (ЕС) № 2016/679.
- (c) Эти Условия не должны истолковываться в нарушение прав и обязанностей, предусмотренных Регламентом (ЕС) № 2016/679.

Условие 5

Преимущественная сила

В случае возникновения противоречий между этими Условиями и положениями соответствующих соглашений между Сторонами, действующих на момент согласования или вступления этих Условий в силу, приоритетное значение имеют настоящие Условия.

Условие 6

Описание передачи или передач данных

Подробная информация о передаче (-ах), в частности категории передаваемых персональных данных и цель (-и) их передачи, указаны в Приложении I.B.

Условие 7 — необязательное

Условие присоединения

- (a) Организация, не являющаяся Стороной настоящих Условий, может с согласия Сторон в любое время присоединиться к этим Условиям как экспортер данных или как импортер данных путем заполнения Дополнения и подписания Приложения I.A.
- (b) После заполнения Дополнения и подписания Приложения I.A. присоединяющаяся организация становится Стороной настоящих Условий и имеет права и обязанности экспортера данных или импортера данных, закрепленные за ней в Приложении I.A.
- (c) Присоединяющаяся организация не имеет прав и обязанностей по этим Условиям, возникшим до того, как она стала Стороной.

РАЗДЕЛ II — ОБЯЗАННОСТИ СТОРОН

Условие 8

Средства защиты данных

Экспортер данных гарантирует, что он сделал все от него зависящее, чтобы убедиться в способности импортера данных выполнить свои обязательства по этим Условиям путем принятия соответствующих организационно-технических мер.

8.1. Указания

- (a) Экспортер данных обязуется обрабатывать персональные данные только в соответствии с документально оформленными указаниями импортера данных, выступающего в качестве их контролера.
- (b) Экспортер данных обязуется немедленно уведомить импортера данных, если не сможет выполнить его указания, в частности если указания противоречат Регламенту (ЕС) № 2016/679 или другому закону ЕС или государства-члена о защите данных.
- (c) Импортер данных не должен совершать никаких действий, которые могут помешать экспортеру данных выполнять его обязательства по Регламенту (ЕС) № 2016/679, в т. ч. касающиеся субобработки или сотрудничества с компетентными надзорными органами.
- (d) После окончания предоставления услуг обработки экспортер данных должен, по усмотрению импортера данных, удалить все персональные данные, обработанные от имени импортера данных, предоставив импортеру данных надежное доказательство такого удаления, или вернуть импортеру данных все обработанные от его имени персональные данные, удалив их копии.

8.2. Безопасность обработки

- (a) Стороны обязуются принять соответствующие организационно-технические меры для обеспечения безопасности данных, в т. ч. во время их передачи, и для предотвращения нарушения безопасности, ведущего к случайному или неправомерному уничтожению, потере, изменению, несанкционированному раскрытию данных или доступу к ним (далее — нарушение безопасности персональных данных). При оценке надежности мер безопасности Стороны должны учитывать технологический уровень,

затраты на внедрение, характер персональных данных ⁽²⁾, характер, объем, условия и цель (-и) обработки, а также риски обработки для субъектов данных, в частности рассматривать возможность использования шифрования или псевдонимизации, в т. ч. во время передачи, если это позволит достигнуть цели обработки.

- (b) Экспортер данных обязан помогать импортеру данных обеспечивать надежную безопасность данных в соответствии с пунктом (а). В случае нарушения безопасности персональных данных, обрабатываемых экспортером данных в соответствии с настоящими Условиями, экспортер данных должен незамедлительно уведомить об этом импортера данных, как только узнает об этом нарушении, и помочь ему устранить последствия нарушения.
- (c) Экспортер данных должен обеспечить, чтобы лица, уполномоченные обрабатывать персональные данные, несли ответственность за соблюдение конфиденциальности по договору или в соответствии с законодательством.

8.3. Документация и соблюдение Условий

- (a) Стороны должны иметь доказательства соблюдения этих Условий.
- (b) Экспортер данных обязан предоставить импортеру данных всю информацию, необходимую для подтверждения соблюдения им своих обязательств в соответствии с настоящими Условиями, а также позволять импортеру данных проводить проверки, содействуя ему в этом вопросе.

Условие 9

Привлечение субобработчиков

Неприменимо

Условие 10

Права субъекта данных

Стороны обязуются помогать друг другу реагировать на запросы и требования субъектов данных, соответствующие положениям местного законодательства, которые относятся к импортеру данных, а в случае обработки данных экспортером данных в ЕС — Регламенту (ЕС) № 2016/679.

Условие 11

Рассмотрение жалоб

- (a) Импортер данных обязан в индивидуальных сообщениях или на своем веб-сайте четко и понятно уведомлять субъектов данных о контактном лице, уполномоченном рассматривать жалобы. Такое лицо незамедлительно рассматривает любые жалобы, поступающие от субъекта данных.

[ВАРИАНТ: Импортер данных соглашается с тем, что субъекты данных также могут бесплатно подавать жалобы в независимый орган

² В ходе этой процедуры определяется, предполагает ли передача и дальнейшая обработка персональных данных раскрытие расовой принадлежности, этнического происхождения, политических взглядов, религиозных или философских убеждений, членства в профсоюзах, генетических или биометрических данных с целью однозначной идентификации физического лица, данных, касающихся здоровья или половой жизни / сексуальной ориентации человека, либо сведений о прошлых судимостях или правонарушениях.

урегулирования споров ⁽³⁾. Импортёр данных должен на условиях, изложенных в пункте (а), уведомлять субъектов данных о таком механизме удовлетворения претензий и о том, что они не обязаны использовать этот механизм или соблюдать определенную последовательность действий при обращении за удовлетворением.]

Условие 12

Ответственность

- (a) Стороны несут друг перед другом ответственность за любой ущерб, причиненный друг другу или другим Сторонам в результате любого нарушения этих Условий.
- (b) Стороны несут ответственность перед субъектом данных, и субъект данных имеет право на получение возмещения любого материального или нематериального ущерба, причиненного ему Стороной в результате нарушения прав стороннего бенефициара, предусмотренных настоящими Условиями. Это положение не ограничивает объем ответственности экспортера данных в соответствии с Регламентом (ЕС) № 2016/679.
- (c) Если в причинении ущерба субъекту данных в результате нарушения этих Условий виновны сразу несколько Сторон, все они несут совместную и индивидуальную ответственность, и субъект данных вправе инициировать судебное разбирательство против любой из этих Сторон.
- (d) Стороны договорились о том, что если в соответствии с пунктом (с) виновной в причинении вреда будет признана только одна Сторона, она имеет право потребовать от другой Стороны или Сторон возмещения ее/их части ущерба.
- (e) Импортёр данных не может ссылаться на действия обработчика или субобработчика в попытке снять с себя ответственность.

Условие 13

Надзор

Неприменимо

РАЗДЕЛ III — МЕСТНОЕ ЗАКОНОДАТЕЛЬСТВО И ОБЯЗАННОСТИ В СЛУЧАЕ ДОСТУПА СО СТОРОНЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Условие 14

Местное законодательство и процессуальные нормы, влияющие на соблюдение Условий

(если обработчик из ЕС объединяет персональные данные, полученные от стороннего контролера, с персональными данными, собранными обработчиком в ЕС)

- (a) Стороны гарантируют, что у них нет оснований полагать, что законодательство и процессуальные нормы третьей страны назначения, распространяющиеся на обработку персональных данных импортёром данных, в частности любые требования раскрытия персональных данных и механизмы, допускающие доступ государственных органов, не позволяют

³ Импортёр данных может предложить независимое урегулирование спора через арбитражный орган при условии, что он учрежден в стране, ратифицировавшей Нью-Йоркскую Конвенцию о признании и приведении в исполнение иностранных арбитражных решений.

импортеру данных выполнять свои обязательства в соответствии с настоящими Условиями. Основанием для этих гарантий является то, что законодательство и процессуальные нормы, в которых учтена сущность основных прав и свобод и которые предусматривают только то, что необходимо и соразмерно в демократическом обществе для защиты одной из целей, установленных в ст. 23(1) Регламента (ЕС) № 2016/679, не противоречат этим Условиям.

- (b) Стороны заявляют, что при предоставлении гарантии, указанной в пункте (a), они внимательно учли различные аспекты, в частности:
 - (i) конкретные обстоятельства передачи, включая длину цепочки обработки, количество задействованных исполнителей и используемые каналы передачи; предполагаемые последующие передачи; тип получателя; цель обработки; категории и формат передаваемых персональных данных; сектор экономики, в котором осуществляется передача; место хранения переданных данных;
 - (ii) законодательство и процессуальные нормы третьей страны назначения, в т. ч. требующие раскрытия данных государственным органам или допускающие их доступ к данным, актуальные при определенных обстоятельствах передачи, а также применимые ограничения и средства защиты ⁽⁴⁾.
 - (iii) все соответствующие договорные и организационно-технические меры предосторожности, принятые в дополнение к средствам защиты, предусмотренным этими Условиями, включая меры, принимаемые во время передачи и обработки персональных данных в стране назначения.
- (c) Импортер данных гарантирует, что при проведении оценки в соответствии с пунктом (b) он сделал все от него зависящее, чтобы предоставить экспортеру данных необходимую информацию, и обязуется продолжать сотрудничество с экспортером данных для обеспечения соблюдения этих Условий.
- (d) Стороны договорились документально оформить результаты оценки, предусмотренной пунктом (b), и предоставить их компетентному надзорному органу по его требованию.
- (e) Импортер данных обязуется незамедлительно уведомить экспортера данных, если после принятия этих Условий в течение срока действия договора у него появятся основания полагать, что он должен соблюдать законодательство и процессуальные нормы, не соответствующие требованиям пункта (a), в частности после изменения законов третьей страны или меры (например, запроса на раскрытие данных), предполагающей применение таких законов на практике в нарушение требований пункта (a).

⁴ Что касается влияния этого законодательства и процессуальных норм на соблюдение этих Условий, в рамках общей оценки могут рассматриваться различные аспекты. В числе этих аспектов может быть актуальный, документально подтвержденный практический опыт обработки запросов государственных органов на раскрытие информации или отсутствие таких запросов за достаточно продолжительный промежуток времени. В частности, это касается удостоверенных высшим руководством внутренних записей или другой документации, ведение которых осуществляется постоянно в целях комплексной проверки благонадежности, если эта информация может передаваться третьим лицам на законных основаниях. Если такой практический опыт планируется использовать исходя из того, что он не помешает импортеру данных соблюдать эти Условия, это допущение должно быть подкреплено другими релевантными и объективными аспектами, и в его поддержку Стороны должны достоверно установить, являются ли эти аспекты вместе взятые достаточно надежными и репрезентативными. В частности, Стороны должны учитывать, соответствует ли их практический опыт и не противоречит ли он общедоступной или иной имеющейся в их распоряжении достоверной информации о наличии или отсутствии запросов в интересующей их отрасли и/или применению закона на практике, например прецедентному праву и отчетам независимых надзорных органов.

- (f) После предоставления уведомления в соответствии с пунктом (е) или если у экспортера данных появятся основания полагать, что импортер данных утратил способность выполнять свои обязательства по этим Условиям, экспортер данных должен незамедлительно определить меры (например, организационно-технические меры для обеспечения безопасности и конфиденциальности), которые должны быть приняты экспортером данных и/или импортером данных для разрешения ситуации. Экспортер данных обязан приостановить передачу данных, если, по его мнению, будет невозможно обеспечить надежные средства защиты для такой передачи или по предписанию компетентного надзорного органа. В таком случае экспортер данных вправе расторгнуть договор в той части, в которой он касается обработки персональных данных, предусмотренной этими Условиями. Если в договоре будут участвовать более двух Сторон, тогда, при отсутствии иной договоренности между ними, экспортер данных может воспользоваться своим правом на расторжение договора только в отношении соответствующей Стороны. В случае расторжения договора в соответствии с этим Условием применяются пункты 16(d) и (е).

Условие 15

Обязанности импортера данных в случае доступа к данным со стороны государственных органов

(если обработчик из ЕС объединяет персональные данные, полученные от стороннего контролера, с персональными данными, собранными обработчиком в ЕС)

15.1. Уведомления

- (a) Импортер данных обязуется незамедлительно уведомить экспортера данных и по возможности субъекта данных (если понадобится, при содействии экспортера данных), если:
- (i) он получит имеющий обязательную силу запрос от государственного органа, включая судебные органы, в соответствии с законодательством страны назначения на раскрытие персональных данных, переданных согласно этим Условиям. В таком уведомлении указывается информация о запрашиваемых персональных данных, органе, от которого поступил запрос, законном основании запроса и ответе на него; или
 - (ii) ему станет известно об осуществлении государственными органами любого прямого доступа к персональным данным, переданным согласно этим Условиям, в соответствии с законодательством страны назначения. В таком уведомлении указывается вся имеющаяся у импортера информация.
- (b) Если законодательство страны назначения запрещает импортеру данных уведомлять экспортера данных и/или субъекта данных, импортер данных обязуется приложить все усилия, чтобы добиться отмены такого запрета и предоставить как можно больше информации в максимально сжатые сроки. Импортер данных обязуется представить документальное свидетельство своих усилий по запросу экспортера данных.

- (с) В случаях, предусмотренных законодательством страны назначения, импортер данных обязуется регулярно в течение срока действия договора предоставлять экспортеру данных как можно больше актуальной информации о поступающих запросах (в частности, об их количестве, типе запрашиваемых данных, запрашивающих органах, о том, были ли запросы оспорены, и о результатах такого оспаривания и т. д.).
- (d) Импортер данных обязуется хранить информацию, предусмотренную пунктами (а) — (с), в течение срока действия договора и предоставлять ее компетентному надзорному органу по его требованию.
- (е) Пункты (а) — (с) не ограничивают обязательство импортера данных по Условию 14(е) и Условию 16 о незамедлительном уведомлении экспортера данных о том, что импортер данных утратил способность соблюдать эти Условия.

15.2. Проверка законности запросов и минимизация данных

- (а) Импортер данных обязуется проверить законность запроса на раскрытие данных, в частности имеет ли государственный орган право направлять такой запрос, и оспорить запрос, если в результате тщательной оценки появятся достаточные основания полагать, что запрос является неправомерным согласно законодательству страны назначения или обязательствам, предусмотренным международными законами и принципами международной вежливости. Импортер данных должен использовать возможности для опротестования запроса на тех же условиях. Оспаривая запрос, импортер данных должен потребовать временного приостановления действия запроса вплоть до принятия решения по существу компетентным судебным органом. Импортер данных не должен раскрывать запрашиваемые персональные данные до тех пор, пока не получит предписание в соответствии с применимыми процессуальными нормами. Эти требования не ограничивают обязательства импортера данных, предусмотренные пунктом 14(е).
- (b) Импортер данных обязуется документально оформить результаты своей правовой оценки и опротестование запроса на раскрытие данных и предоставить документацию экспортеру данных в объеме, предусмотренном законодательством страны назначения. Кроме того, импортер данных должен предоставить документацию компетентному надзорному органу по его требованию.
- (с) Импортер данных обязуется предоставить минимально допустимый объем информации в ответе на запрос на раскрытие данных с учетом его разумно обоснованной интерпретации.

РАЗДЕЛ IV — ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Условие 16

Несоблюдение Условий и прекращение действия

- (а) Импортер данных должен незамедлительно уведомить экспортера данных, если он по какой-либо причине утратит способность выполнять эти Условия.

- (b) Если импортер данных нарушит эти Условия или не сможет их соблюдать, экспортер данных остановит передачу персональных данных импортеру данных до тех пор, пока импортер данных не возобновит соблюдение Условий или пока не будет расторгнут договор. Данное требование не противоречит пункту 14(f).
- (c) Экспортер данных вправе расторгнуть договор в той части, в которой он касается обработки персональных данных, предусмотренной этими Условиями, если:
 - (i) экспортер данных приостановит передачу персональных данных импортеру данных в соответствии с пунктом (b) и соблюдение этих Условий не будет возобновлено в приемлемый срок, но в любом случае в течение одного месяца после приостановки передачи;
 - (ii) импортер данных будет постоянно или существенно нарушать эти Условия; или
 - (iii) импортер данных не выполнит обязательное постановление компетентного суда или надзорного органа, касающееся его обязательств по этим Условиям.

В любом таком случае импортер данных должен уведомить компетентный надзорный орган о несоблюдении настоящих Условий. Если в договоре будут участвовать более двух Сторон, тогда, при отсутствии иной договоренности между ними, экспортер данных может воспользоваться своим правом на расторжение договора только в отношении соответствующей Стороны.

- (d) Персональные данные, собранные экспортером данных в ЕС, которые были переданы до расторжения договора в соответствии с пунктом (c), в т. ч. любые их копии, подлежат немедленному и полному удалению. Импортер данных должен предоставить экспортеру данных доказательства удаления таких данных. До удаления или возврата данных импортер данных обязан продолжать соблюдение этих Условий. Если возврат или удаление переданных персональных данных запрещен местным законодательством, действие которого распространяется на импортера данных, в таком случае импортер данных обязан продолжать соблюдение этих Условий и обрабатывать данные в объеме и в течение срока, предусмотренных местным законодательством.
- (e) Любая из Сторон вправе отозвать свое согласие на соблюдение этих Условий, если: (i) Европейская комиссия примет решение в соответствии со ст. 45(3) Регламента (ЕС) № 2016/679, касающееся передачи персональных данных, на которые распространяются эти Условия; или (ii) Регламент (ЕС) № 2016/679 станет частью правовой системы страны, в которую передаются персональные данные. Это положение не ограничивает объем других обязательств, применимых к указанной обработке данных в соответствии с Регламентом (ЕС) № 2016/679.

Условие 17

Применимое законодательство

Эти Условия регулируются национальным законодательством, допускающим права сторонних бенефициаров. Стороны договорились о том, что это будет законодательство _____ (указать страну).

Условие 18

Выбор места урегулирования споров и юрисдикции

Любой спор, возникающий в связи с настоящими Условиями, рассматривается в судах _____ (указать страну) **ДОПОЛНЕНИЕ**

ПОЯСНЕНИЯ

Должна быть возможность четко различать информацию, применимую к каждой передаче или категории передач, и в связи с этим определять соответствующую функцию или функции Сторон как экспортеров данных и/или импортеров данных. Если подобную прозрачность можно обеспечить с помощью одного дополнения, необязательно оформлять и подписывать отдельные приложения по каждой передаче/категории передач и/или договорным отношениям. Однако если необходимо гарантировать достаточную четкость, следует использовать отдельные дополнения.

ПРИЛОЖЕНИЕ I

А. СПИСОК СТОРОН

Экспортер (-ы) данных: *[Наименование и контактные данные экспортера (-ов) данных и, если применимо, его/их директора по защите персональных данных и/или представителя в Европейском союзе]*

1.

Наименование: _____

Адрес: _____

Имя и фамилия, должность и контактные данные контактного лица: _____

Действия с данными, передаваемыми в соответствии с этими Положениями: _____

Подпись и дата: _____

Функция (контролер/обработчик): _____

2.

Импортер (-ы) данных: *[Наименование и контактная информация импортера (-ов) данных, включая контактное лицо, ответственное за защиту данных]*

1.

Наименование: _____

Адрес: _____

Имя и фамилия, должность и контактные данные контактного лица: _____

Действия с данными, передаваемыми в соответствии с этими Положениями: _____

Подпись и дата: _____

Функция (контролер/обработчик): _____

В. ОПИСАНИЕ ПЕРЕДАЧИ

Категории субъектов данных, персональные данные которых подлежат передаче

Категории передаваемых персональных данных

Передаваемые конфиденциальные данные (если применимо) и используемые ограничения или меры предосторожности, полностью учитывающие характер данных и связанные с ними риски, в частности строгое ограничение цели, ограничения доступа (в т. ч. доступ только для персонала, прошедшего специальное обучение), учет доступа к данным, ограничения последующих передач и дополнительные меры безопасности.

Периодичность передачи данных (например, один раз или постоянно).

Характер обработки

Цель (-и) передачи и дальнейшей обработки данных

Срок хранения персональных данных, а если он неизвестен, критерии его определения

В случае передач данных (суб)обработчикам также следует указать предмет, характер и продолжительность обработки

Приложение В: Поправки к СДУ ЕС для конкретных стран

Швейцария

Для целей Закона о защите данных Швейцарии, если передача Персональных данных клиентов на основании ЛСКП регулируется GDPR и Законом о защите данных Швейцарии, Условия передачи О — К применяются в случаях, установленных разделами 8.1. и 8.2. настоящего СОД, с изложенными ниже поправками (во избежание двусмысленного толкования эти поправки не влияют на Условия передачи О — К, применимые для целей GDPR):

- Упоминания о Регламенте (ЕС) № 2016/679 или слова «этот Регламент» означают упоминания о Законе о защите данных Швейцарии в применимом объеме.
- Упоминания о Регламенте (ЕС) № 2018/1725 удалены.
- Слова «Союз», «ЕС» и словосочетание «Государство — член ЕС» следует толковать как Швейцарию.
- Положение 17 изменено и имеет следующую формулировку: «Эти Положения регулируются законодательством Швейцарии в объеме, в котором Закон о защите данных Швейцарии применяется к передачам данных».
- Положение 18 изменено и имеет следующую формулировку:

«Все споры, возникающие в результате этих Положений и связанные с Законом о защите данных Швейцарии, передаются на рассмотрение в суды Швейцарии. Субъект данных может также подать иск против экспортера и/или импортера данных в суды Швейцарии по месту своего жительства. Стороны обязуются подчиняться юрисдикции этих судов».
- До вступления в силу пересмотренного Закона о защите данных Швейцарии Условия передачи О — К также применяются для защиты персональных данных юридических лиц, причем в соответствии с Условиями передачи О — К юридические лица должны иметь такую же защиту, что и физические лица.

Для целей Закона о защите данных Швейцарии, если передача Персональных данных клиентов на основании ЛСКП регулируется исключительно Законом о защите данных Швейцарии, Условия передачи О — К применяются в случаях, установленных разделами 8.1. и 8.2. настоящего СОД, с указанными ниже поправками:

- Упоминания о Регламенте (ЕС) № 2016/679 или слова «этот Регламент» следует толковать как упоминания Закона о защите данных Швейцарии.
- Упоминания о Регламенте (ЕС) № 2018/1725 удалены.
- Слова «Союз», «ЕС» и словосочетание «Государство — член ЕС» следует толковать как Швейцарию.
- Положение 17 изменено и имеет следующую формулировку: «Эти Положения регулируются законодательством Швейцарии».
- Положение 18 изменено и имеет следующую формулировку:

«Все споры, возникающие в результате этих Положений и связанные с Законом о защите данных Швейцарии, передаются на рассмотрение в

суды Швейцарии. Субъект данных может также подать иск против экспортера и/или импортера данных в суды Швейцарии по месту своего жительства. Стороны обязуются подчиняться юрисдикции этих судов».

- До вступления в силу пересмотренного Закона о защите данных Швейцарии Условия передачи О — К также применяются для защиты персональных данных юридических лиц, причем в соответствии с Условиями передачи О — К юридические лица должны иметь такую же защиту, что и физические лица.

Приложение С: Описание передачи

Категории субъектов данных, персональные данные которых подлежат передаче

К субъектам данных относятся физические лица, данные которых предоставляются компании Pix4D через Лицензированные предложения Вами (или по Вашему указанию) или Авторизованными пользователями, включая третьих лиц, фигурирующих в Контенте.

Категории передаваемых персональных данных

Данные о физических лицах, предоставляемые компании Pix4D через Услуги Вами (или по Вашему указанию) или Авторизованными пользователями, включая персональные данные третьих лиц, фигурирующих в Контенте.

Передаваемые конфиденциальные данные (если применимо) и используемые ограничения или меры предосторожности, полностью учитывающие характер данных и связанные с ними риски, в частности строгое ограничение цели, ограничения доступа (в т. ч. доступ только для персонала, прошедшего специальное обучение), учет доступа к данным, ограничения последующих передач и дополнительные меры безопасности:

Стороны не планируют осуществлять передачу конфиденциальных данных.

Периодичность передачи данных (например, один раз или постоянно):

Регулярно и постоянно.

Характер обработки:

Компания Pix4D будет обрабатывать Персональные данные клиентов с целью предоставления Лицензированного предложения для использования Вами и Авторизованными пользователями в соответствии с ЛСКП.

Цель (-и) передачи и дальнейшей обработки данных:

Срок хранения персональных данных, а если он неизвестен, критерии его определения

Срок действия плюс промежуток времени с даты окончания Срока действия по дате удаления всех Данных клиентов компанией Pix4D в соответствии с ЛСКП и этим СОД.

В случае передач данных (суб)обработчикам также следует указать предмет, характер и продолжительность обработки

См. список субобработчиков компании Pix4D, опубликованный на веб-странице <https://www.pix4d.com/legal>.

Приложение D: Меры безопасности

Ниже изложены организационно-технические меры (в т.ч. все необходимые сертификаты), внедренные компанией Pix4D для обеспечения надлежащего уровня безопасности (далее — **Меры безопасности**) с учетом характера, объема, условий и цели обработки данных, а также рисков для прав и свобод субъектов данных:

1. Меры псевдонимизации и шифрования персональных данных
 - a) Псевдонимизация осуществляется так, чтобы данные было невозможно соотнести с конкретным субъектом данных без дополнительной информации.
 - b) Дополнительная информация, необходимая для соотнесения персональных данных с конкретным субъектом данных, хранится в отдельных надежно защищенных системах, доступ к которым имеет ограниченный круг лиц.
 - c) При шифровании персональных данных используются алгоритмы и длина ключей, соответствующие степени конфиденциальности данных.
 - d) Шифровальные ключи хранятся в надежно защищенном месте и выдаются только ограниченному кругу лиц.
 - e) Система внутренних директив гарантирует выполнение анонимизации/псевдонимизации по мере возможности на случай раскрытия данных или даже после истечения установленного законом срока их удаления.
2. Меры по обеспечению конфиденциальности, целостности, доступности и отказоустойчивости систем и сервисов обработки данных
 - a) Ответственность за координацию и мониторинг правил и процедур информационной безопасности несет сотрудник службы безопасности или назначенный член высшего руководства.
 - b) Аспекты защиты данных являются неотъемлемой частью корпоративного управления рисками.
 - c) На объектах, где расположены информационные системы, обрабатывающие персональные данные, реализуются планы действий в чрезвычайных ситуациях и при возникновении непредвиденных обстоятельств.
 - d) По мере необходимости проводится оценка последствий для защиты данных (data protection impact assessment, DPIA).
 - e) Сотрудники прошли соответствующее обучение и несут ответственность за соблюдение конфиденциальности и секретности данных.
 - f) Сотрудники уведомлены об их функциях и соответствующих процедурах безопасности.
 - g) Сотрудники уведомлены о возможных последствиях нарушения правил и процедур безопасности.

- h) Сотрудники получают рабочие указания касательно контроля доступа, коммуникационной и операционной безопасности.
 - i) В рабочих указаниях подробно изложены меры безопасности, соответствующие процедуры и обязанности.
 - j) Все правила, инструкции и руководства по защите персональных данных документально оформлены на центральном уровне и доступны каждому сотруднику.
 - k) Критические компоненты системы находятся под постоянным контролем специализированных систем, обеспечивающих их защиту от пожара, воды, влажности, ударов, тепла, холода и непредвиденного отключения электроэнергии.
 - l) Критические компоненты системы допускают возможность их быстрой замены в случае выхода из строя, например с помощью резервных компонентов, RAID-систем или зеркалирования данных.
 - m) При необходимости для операционных систем и данных используются отдельные разделы.
3. Меры по обеспечению своевременного восстановления работоспособности и доступа к персональным данным в случае физической поломки или технического сбоя
- a) Стратегия резервного копирования определяется по количеству данных и периодичности их изменения.
 - b) Стратегия резервного копирования предназначена для восстановления персональных данных до состояния, в котором они были на момент потери или уничтожения.
 - c) Системы резервного копирования физически изолированы от производственных систем.
 - d) На серверах резервного копирования используются те же меры безопасности, что и на рабочих серверах.
 - e) Лица, ответственные за восстановление данных, прошли специальное обучение выполнению этой задачи.
4. Процедуры регулярного тестирования, оценки и анализа эффективности организационно-технических мер (ОТМБ) для обеспечения безопасности обработки данных
- a) Эффективность ОТМБ оценивается с определенной периодичностью импортером данных. Характер и частотность оценок определяются по используемой мере.
 - b) Если результаты оценки показывают, что ОТМБ не внедрены вообще или внедрены в недостаточном объеме либо не обеспечивают требуемой эффективности, определяются и принимаются соответствующие меры.

- c) Если результаты оценки существующих ОТМБ показывают, что их уже недостаточно (например, в случае появления новых угроз), внедряются новые ОТМБ.
 - d) Для постоянного мониторинга эффективности ОТМБ и координирования оценок и подлежащих внедрению мер назначается одно или несколько ответственных лиц.
5. Меры по идентификации и авторизации пользователей
- a) Доступ к информационным системам защищен стандартными процедурами идентификации и аутентификации.
 - b) Устройства хранения данных, рабочие станции, ноутбуки, смартфоны и планшеты защищены с помощью стандартных методов шифрования.
 - c) Управление учетными записями пользователей и их разрешениями осуществляется ответственными лицами (администраторами).
 - d) Ограничительные модели авторизации прав на базы данных, действующие по принципу служебной необходимости, управляются минимальным количеством администраторов.
 - e) Доступ к персональным данным предоставляется только сотрудникам, у которых имеется законная потребность в нем для выполнения ими своих конкретных должностных обязанностей.
 - f) Обеспечена возможность обработки данных, собранных для разных целей, отдельно от других данных.
 - g) Запрещены действия в системе без авторизованного доступа.
 - h) Руководства разработаны и оформлены по темам: «безопасные пароли», «удаление/уничтожение данных», «чистый стол», «мобильное устройство».
 - i) Все учетные записи пользователей, допускающие аутентификацию, являются персональными и используются только одним человеком.
 - j) Сотрудники уведомлены о необходимости завершать административные сеансы, когда они покидают помещение или когда рабочие станции остаются без присмотра по иным причинам.
 - k) Пароли пользователей состоят как минимум из восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы.
 - l) Для доступа к критическим системам используется двухфакторная аутентификация.
 - m) Шредер файлов и/или внешний уничтожитель файлов соответствуют стандарту безопасности DIN 66399.
6. Меры по защите персональных данных во время их передачи
- a) Удаленный доступ осуществляется только через зашифрованные каналы (VPN).

- b) Электронная передача данных и передача персональных данных осуществляется с помощью стандартных для отрасли методов шифрования. Для электронной почты по возможности используется как минимум линейное шифрование (TLS).
 - c) При необходимости применяются процедуры сертификации цифровой подписью.
 - d) Данные не передаются неопознанным третьим лицам.
7. Меры по защите данных во время их хранения
- a) Доступ к конкретным данным предоставляется только лицам, ответственным за их обработку. Этот процесс контролируется посредством модели авторизации пользователей.
 - b) При необходимости разные данные клиентов хранятся в разных базах данных.
 - c) Внешние носители, содержащие конфиденциальные персональные данные, защищены с помощью шифрования и физических средств.
 - d) Право на ввод, изменение и удаление данных предоставляется на основании модели полномочий.
 - e) Право на стирание данных предоставляется в ограниченном объеме.
8. Меры по обеспечению физической безопасности мест обработки персональных данных
- a) Системы и сервисы защищены от случайного или незаконного уничтожения, случайной потери, изменения, несанкционированного раскрытия или доступа.
 - b) Установлена круглосуточная охранная сигнализация.
 - c) Наружные и межкомнатные двери оснащены магнитными и замыкающими контактами.
 - d) Все ключи и ключ-карты именные.
 - e) В рабочее время на входе и в приемной зоне всегда находятся соответствующие сотрудники.
 - f) Здания и входы в них находятся под постоянным видеонаблюдением.
 - g) Посетителей всегда сопровождают сотрудники.
 - h) Выполняется тщательный отбор сторонних специалистов.
 - i) Если системы размещаются, управляются и обслуживаются внешними поставщиками услуг, принимаются соответствующие меры по обеспечению этими поставщиками услуг надлежащих мер безопасности.
9. Меры по обеспечению регистрации событий
- a) Отслеживаются и регистрируются авторизация доступа и получение данных.

- b) Регистрируется выдача ключей и ключ-карт.
 - c) Регистрируется доступ посетителей.
 - d) Регистрируется ввод, изменение и удаление данных.
 - e) Регистрируются меры по восстановлению данных.
 - f) Регистрируются результаты оценки эффективности ОТМБ.
 - g) Регистрируются результаты проверки структуры отчетов.
 - h) Регистрируются инциденты в области безопасности и нарушения безопасности данных. Ведутся записи о характере нарушения безопасности данных, категориях и приблизительном количестве субъектов данных и записей персональных данных, затронутых нарушением, сроке его действия и последствиях, процедуре восстановления данных, мерах, принятых для минимизации неблагоприятных последствий, а также регистрируются имена и фамилии лиц, сообщивших о нарушении безопасности данных, и лиц, получивших эту информацию.
 - i) Журналы позволяют отслеживать не группы пользователей, а каждого отдельного пользователя.
10. Меры по обеспечению конфигурации системы, в т. ч. конфигурации по умолчанию
- a) Принимаются технические меры, позволяющие субъектам данных легко реализовать свое право отозвать разрешения на обработку их данных.
 - b) В стандартном и специальном программном обеспечении используются настройки по умолчанию, которыми удобно пользоваться для защиты данных.
11. Меры защиты внутренней ИТ-системы и управления ИТ-безопасностью
- a) На серверах и программах-клиентах установлено антивирусное программное обеспечение и брандмауэр, защищающие от несанкционированного доступа к системам, осуществляемого с помощью вредоносных программ.
 - b) Работает система обнаружения вторжений.
 - c) Внедрен официальный план действий при инцидентах в области безопасности.
 - d) Осуществляется контроль удаленного доступа посторонних лиц.
 - e) Аппаратное и программное обеспечение ИТ-системы проверяется с конкретной периодичностью для определения необходимости их обновления или замены из соображений безопасности.
12. Меры по сертификации/контролю качества процессов и продуктов
- a) Проводятся регулярные оценки необходимости сертификации систем и продуктов.

- b) Регулярно выполняется сертификация безопасности данных (если применимо) и аудиты (включая испытания на проникновение, в соответствующих случаях).

13. Меры по обеспечению минимизации данных

- a) Сбор персональных данных осуществляется только в объеме, необходимом для достижения поставленных целей.
- b) Персональные данные периодически проверяются и удаляются, если они больше не используются и если позволяют законные/договорные положения.

14. Меры по обеспечению качества данных

- a) При необходимости выполняется проверка ввода данных на достоверность.
- b) При необходимости пользователям предоставляется возможность проверить введенные ими данные.

15. Меры по обеспечению ограниченного хранения данных

- a) По возможности и если это целесообразно, устанавливаются сроки хранения данных.
- b) По возможности и если это целесообразно, к документам и данным, хранящимся в производственных системах, применяются протоколы автоматического архивирования.

16. Меры по обеспечению отчетности

- a) Определена формальная процедура отслеживания инцидентов в области безопасности и нарушения безопасности данных.
- b) Механизмы контроля соблюдения принципов защиты данных основываются на требованиях применимого законодательства о защите персональных данных.
- c) Структуры отчетности согласуются с организацией Группы и соответствующего подразделения и позволяют принимать ответные меры оперативно и, если применимо, в предусмотренные законом сроки.
- d) Выполняются регулярные проверки эффективности структур отчетности с предварительно заданными интервалами.
- e) Если результаты оценки показывают, что структуры отчетности не внедрены вообще или внедрены в недостаточном объеме либо не обеспечивают требуемой эффективности, определяются и принимаются соответствующие меры.

17. Меры по обеспечению переносимости и стирания данных

- a) Четко определены обязанности в отношении переносимости данных.
- b) Действуют формальные процедуры обработки запросов на переносимость данных.

- c) Предусмотрена возможность идентификации и разделения наборов данных с помощью функций выбора используемой системы.
- d) Запросы на переносимость данных незамедлительно отправляются в соответствующие подразделения, и по ним сразу принимаются меры с целью соблюдения установленных законом сроков.
- e) Для обеспечения удаления персональных данных из систем Поставщика после расторжения Основного соглашения принимаются соответствующие меры.
- f) Лица, ответственные за переносимость данных, обладают квалификацией и опытом, необходимыми для обработки запросов. В частности, четко определяется, какая именно информация подлежит раскрытию, передаче или удалению и какие запросы или их части не должны выполняться.
- g) Персональные данные передаются безопасными средствами в четко организованных, широко используемых машиночитаемых форматах.