ПОСЛЕДНЕЕ ОБНОВЛЕНИЕ: 22 июня 2021 г.

Дополнение по обработке данных

Настоящее Дополнение по обработке данных («**DPA**») является дополнением к Лицензионному соглашению конечного пользователя Lincoln Electric Company («**ЛСКП**») и применяется между Lincoln Electric Company («**Оператор данных**») и Авторизованным пользователем в соответствии с ЛСКП («**Контролер данных**»), (каждый из которых является «**Стороной**», а совместно — «**Сторонами**»).

В СВЯЗИ С ТЕМ, ЧТО

ЛСКП регулирует право Авторизованного пользователя использовать Лицензированное приложение и, если применимо, другие онлайн-сервисы, предоставляемые компанией Lincoln Electric. Для выполнения своих обязательств по ЛСКП компания Lincoln Electric Company должна действовать как Оператор данных от имени Авторизованного пользователя. Чтобы обеспечить соблюдение правил в отношении персональных данных, Стороны договорились дополнить ЛСКП, изложив условия, применимые к обработке персональных данных Оператором данных от имени Контролера данных.

НАСТОЯЩИМ СТОРОНЫ СОГЛАШАЮТСЯ О НИЖЕСЛЕДУЮЩЕМ

1. ОПРЕДЕЛЕНИЯ

1.1 В данном DPA термины, написанные с заглавной буквы, имеют следующие значения, если они не определены в ЛСКП или иным образом не требуются с учетом контекста:

«**Контролер данных»**	означает субъекта, определяющего цели и средства Обработки Персональных данных;
«Оператор данных»	означает субъекта, который обрабатывает персональные данные от имени Контролера данных;
«Субъект данных»	означает идентифицированное или идентифицируемое лицо, чьи Персональные данные обрабатываются;
«Инструкция»	означает инструкции, предоставленные Контролером данных Оператору данных для обработки Персональных данных в соответствии с предоставлением услуг в соответствии с ЛСКП;
«Персональные данные»	означает любую информацию, относящуюся к идентифицированному или идентифицируемому лицу. Идентифицируемое лицо — это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на такие идентификаторы как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор, или на один или несколько факторов, специфичных для его или ее физической, физиологической, генетической, ментальной, экономической, культурной или социальной идентичности;
«Нарушение правил защиты персональных данных»	означает нарушение безопасности, ведущее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к Персональным данным, переданным, хранящимся или обрабатываемым иным образом;
«Обработка» / «Порядок обработки» / «Обработано»	означает любое действие, выполняемое с Персональными данными, такое как сбор, запись, организация, хранение, адаптация или изменение, извлечение, консультация, использование, раскрытие путем пересылки, распространения, передачи или иного предоставления доступа, согласования или комбинации, ограничения, удаления или уничтожения;
«Услуги по обработке»	означает обработку Персональных данных Оператором данных в связи с ЛСКП;
«Особые категории личных данных»	означает любые Персональные данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или

философские убеждения или членство в профсоюзе, ассоциациях или фондах, внешний вид, судимости и меры безопасности, финансовую и имущественную информацию, информацию о местонахождении или кредитную информацию, а также Обработку генетических данных, биометрических данных с целью однозначной идентификации физического лица, данных о его здоровье или данных, касающихся его половой жизни или сексуальной ориентации, или данных о несовершеннолетних в возрасте 14 лет и младше;

«Стандартные договорные положения» означает стандартные договорные положения, принятые Решением Комиссии ЕС 2010/87 от 5 февраля 2010 г., о стандартных договорных положениях для передачи персональных данных операторам, установленным в третьих странах, или любой альтернативный набор стандартных положений, согласованный между Сторонами. Если Контролер данных учрежден в юрисдикции за пределами Европейского Союза, ссылки на государства-члены в основных положениях Стандартных договорных условий должны толковаться как ссылки на юрисдикцию, в которой учрежден Контролер данных;

«Субоператор» означает любого оператора, привлеченного Оператором данных (или любым другим Субоператором Оператора данных) для Обработки Персональных данных от имени Контролера данных в соответствии с его Инструкциями и условиями письменного субподряда.

1.2 Заголовки и подзаголовки разделов используются только в справочных целях и для удобства. Они не являются частью настоящего DPA и не должны использоваться при его толковании.

2. ОБЪЕМ И ПРИМЕНЕНИЕ ДАННОГО DPA

2.1 Это DPA только дополняет положения ЛСКП в отношении Услуг по обработке, предоставляемых Оператором данных Контролеру данных в соответствии с ЛСКП.

3. ОБРАБОТКА ДАННЫХ

3.1 Оператор данных соглашается обрабатывать Персональные данные в соответствии с условиями, изложенными в этом DPA. В частности, Оператор данных обязуется:

3.1.1 обрабатывать Персональные данные только от имени Контролера данных и в любое время в соответствии с Инструкциями Контролера данных, как определено в этом DPA, и всеми действующими законами о защите данных;

3.1.2 гарантировать, чтобы персонал, которому доверены Услуги по обработке, взял на себя обязательство соблюдать конфиденциальность или действовал в соответствии с установленным законом обязательством конфиденциальности;

3.1.3 принимать технические, физические и организационные меры для обеспечения безопасности и конфиденциальности Персональных данных и надлежащим образом защищать Персональные данные, обрабатываемые от имени Контролера данных, от неправомерного использования и потери, как предусмотрено в Приложении 2 настоящего DPA;

3.1.4 незамедлительно уведомлять Контролера данных о: (a) любом имеющем обязательную юридическую силу запросе о раскрытии Персональных данных государственным органом, если иное не запрещено, например, о запрете в соответствии с уголовным законодательством для сохранения конфиденциальности расследования правоохранительных органов или разведки, (b) любом нарушении персональных данных, затрагивающем Персональные данные, обрабатываемые от имени Контролера данных, (c) любом запросе, полученном непосредственно от Субъектов данных (включая права на доступ, исправление, удаление, возражение, ограничение, передачу данных и право не регулироваться решениями, основанными исключительно на автоматизированной Обработке, включая профилирование); Оператор данных (i) не должен отвечать напрямую на этот запрос, за исключением уведомления

Субъекта данных о том, что он действует от имени Контролера данных, и предоставления Субъекту данных контактной информации Контролера данных, и (ii) принимая во внимание характер Обработки, будет оказывать помощь Контролеру данных соответствующими техническими, физическими и организационными мерами, насколько это возможно, для выполнения обязанности Контролера данных отвечать на запросы об осуществлении прав Субъекта данных;

3.1.5 обеспечить коммерчески разумное сотрудничество с Контролером данных, чтобы помочь Контролеру данных выполнить свои собственные юридические обязательства, связанные с безопасностью Персональных данных, такие как уведомление о нарушении защиты Персональных данных в компетентный надзорный орган, сообщение о таком нарушении защиты Персональных данных в затронутые Субъекты данных и, где это применимо, проведение оценок воздействия на защиту данных и предварительные консультации с надзорными органами с учетом характера Обработки и информации, доступной Оператору данных;

3.1.6 предоставить Контролеру данных всю информацию, необходимую для подтверждения соблюдения обязательств, изложенных в этом DPA, а также разрешить и вносить свой вклад в аудит, включая проверки, проводимые Контролером данных или другим аудитором, уполномоченным Контролером данных, как указано в Разделе 6; а также

3.1.7 что любые услуги по обработке, выполняемые Субоператором, должны осуществляться в соответствии с Разделом 7.

3.2 Что касается Услуг по обработке, Контролер данных будет нести ответственность за соблюдение всех требований, которые применяются к нему в соответствии с применимым законодательством в отношении Обработки Персональных данных и Инструкций, которые он передает Оператору данных. В частности, но без ущерба для общего характера вышеизложенного, Контролер данных признает и соглашается с тем, что он будет нести единоличную ответственность за следующее: (i) точность, качество и законность Персональных данных; (ii) соблюдение всех необходимых требований прозрачности и законности в соответствии с применимым законодательством для сбора и использования Персональных данных, включая получение любых необходимых разрешений и разрешений от Субъектов данных или иным образом; (iii) обеспечение права Контролера данных передавать или предоставлять доступ к Персональным данным Оператору данных, а также предоставления Контролером данных всех необходимых уведомлений и получения всех необходимых согласий и (или) разрешений в отношении такой передачи или доступа и, в более общем плане, для Обработки в соответствии с условиями ЛСКП (включая это DPA); а также (iv) обеспечение соответствия Инструкций действующему законодательству. По запросу Оператора данных Контролер данных должен предоставить Оператору данных в течение трех (3) рабочих дней письменное подтверждение таких уведомлений, согласий и разрешений. Контролер данных не должен вводить в Услуги по обработке какие-либо особые категории Персональных данных или иным образом предоставлять их Оператору данных, если Контролер данных отдельно не договорился об ином в письменной форме. Контролер данных незамедлительно и без неоправданной задержки должен проинформировать Оператора данных о невозможности Контролера данных выполнить свои обязанности, изложенные в этом DPA. Авторизованный пользователь несет исключительную ответственность за пересмотр Услуг по обработке, включая любую доступную документацию и функции безопасности, чтобы определить, удовлетворяют ли они требованиям, бизнес-потребностям и юридическим обязательствам Авторизованного пользователя.

3.3 Контролер данных разрешает Оператору данных анонимизировать Персональные данные, обрабатываемые в соответствии с ЛСКП, для получения аналитических данных, касающихся использования Лицензированного приложения, продуктов и оборудования компании Lincoln. Дальнейшее использование полученных статистических данных Оператором данных не требует предварительного разрешения от Контролера данных.

4. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ДАННЫХ

4.1 Контролер данных настоящим подтверждает и соглашается с тем, что для предоставления Услуг по обработке в соответствии с ЛСКП Оператор данных может передавать Персональные данные в Соединенные Штаты Америки и в любую другую страну, в которой находится Оператор данных, и хранить их там для целей предоставления Услуг по обработке. Таким образом, в процессе

предоставления Услуг по обработке может возникнуть необходимость в передаче Персональных данных Оператору данных, находящемуся за пределами страны учреждения Контролера данных. Если Контролер данных находится в Европейской экономической зоне или в Швейцарии, Стороны обязуются применять положения Стандартных договорных условий для передачи Персональных данных Контролером данных (действующим как экспортер данных в соответствии со Стандартными договорными условиями) Оператору данных (действующему как импортер данных в соответствии со Стандартными договорными условиями).

4.2 Если Контролер данных находится за пределами Европейской экономической зоны и Швейцарии, Стороны также обязуются применять положения Стандартных договорных условий для передачи Персональных данных Контролером данных (действующим как экспортер данных в соответствии со Стандартными договорными условиями) Оператору данных (действующему как импортер данных в соответствии со Стандартными договорными положениями) при условии, что Стандартные договорные положения требуются по закону и достаточны для выполнения требований применимых правил защиты данных для передачи Персональных данных Контролером данных Оператору данных в соответствии с ЛСКП.

4.3 Если Стороны применяют Стандартные договорные условия в соответствии с Разделами 4.1 или 4.2 настоящего DPA:

4.3.1 Приложение 1 Стандартных договорных условий применяется на следующей основе: (a) экспортер данных: Контролер данных, (b) импортер данных: Оператор данных, (c) Субъекты данных: персонал Контролера данных (Авторизованный пользователь), (d) Категории данных: данные, касающиеся использования продуктов и оборудования, принадлежащих, лицензированных или управляемых Оператором данных, которые отслеживаются Лицензированным приложением в соответствии с ЛСКП, включая регистрационные данные (т. е. имена пользователей и пароли), (e) Особые категории Персональных данных: не применимо, а также (f) Операции обработки: сбор, копирование, передача, хранение, изменение, удаление и другие операции, необходимые для Услуг по обработке в соответствии с ЛСКП.

4.3.2 Описание технических, физических и организационных мер безопасности, реализуемых Оператором данных, выступающим как импортер данных для целей Приложения 2 Стандартных договорных условий, должно соответствовать Приложению 2 к настоящему DPA.

4.4 Если Стандартные договорные положения применимы к Сторонам в соответствии с Разделом 4.1 или 4.2, их положения будут считаться включенными посредством ссылки в настоящее DPA, если только Стороны не оформят Стандартные договорные положения как отдельный документ в соответствии с Разделом 4.5.

4.5 В той степени, в которой это требуется применимыми правилами защиты данных, Стороны заключают и исполняют Стандартные договорные положения как отдельный документ.

5. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ СОГЛАШЕНИЯ

5.1 Это DPA вступает в силу с даты вступления в силу ЛСКП.

5.2 Это DPA будет автоматически прекращено после прекращения или истечения срока действия (a) ЛСКП или (b) обязательств Оператора данных в отношении Услуг по обработке, и такое прекращение не требует постановления суда, судебного разбирательства или любых других действий со стороны Оператора данных, Контролера данных или любой другой стороны для обеспечения эффективности. В соответствующих случаях после прекращения действия настоящего DPA Оператор данных должен вернуть Контролеру данных или удалить, по запросу Контролера данных, все Персональные данные Контролера данных, находящиеся в его владении или под его контролем. По требованию Контролера данных, Оператор данных должен подтвердить соблюдение таких обязательств в письменной форме и удалить все существующие копии, если действующее законодательство не требует хранения или иным образом не разрешает хранение Персональных данных.

5.3 Контролер данных имеет право расторгнуть настоящее DPA путем письменного уведомления Оператора данных, если Оператор данных существенно или постоянно нарушает данное DPA и если это является таким нарушением, которое можно устранить, но которое не было устранено в течение тридцати (30)

рабочих дней с даты получения Оператором данных уведомления от Контролера данных с указанием на нарушение и требованием его устранения.

5.4 Оператор данных имеет право прекратить действие настоящего DPA путем письменного уведомления Контролера данных, если Контролер данных существенно или постоянно нарушает данное DPA и если это является таким нарушением, которое можно устранить, но которое не было устранено в течение тридцати (30) рабочих дней с даты получения Контролером данных уведомления от Оператора данных с указанием на нарушение и требованием его устранения.

6. АУДИТ И ИНФОРМАЦИОННЫЕ ЗАПРОСЫ

6.1. В пределах одного (1) аудита в год и при условии уведомления Контролером данных с предварительным уведомлением за тридцать (30) дней, за исключением случая аудита, запрошенного надзорным органом, Контролер данных может в обычное рабочее время, без необоснованного вмешательства в бизнес-операции Оператора данных, лично проверять Оператора данных или назначать стороннего аудитора, который несет обязательства по соблюдению конфиденциальности для проведения такого аудита.

6.2. Оператор данных должен проявлять сотрудничество в случае аудита в соответствии с настоящим Разделом 6 и предоставлять Контролеру данных всю информацию, необходимую для проведения такого аудита. Контролер данных покрывает расходы и издержки, понесенные каждой стороной в связи с аудитами в соответствии с настоящим Разделом 6.

7. НАЗНАЧЕНИЕ СУБОПЕРАТОРОВ

7.1 Контролер данных разрешает Оператору данных использовать услуги Субоператоров, перечисленных на странице, доступной по адресу [https://www.lincolnelectric.com/en/Legal-Information/Subprocessors], исключительно в соответствии с требованиями для оказания Услуг в связи с ЛСКП.

7.2 Контролер данных разрешает Оператору данных использовать услуги новых Субоператоров при условии предварительного уведомления Контролера данных Оператором данных с уведомлением за пятнадцать (15) дней до смены Субоператора. Если Контролер данных возражает против изменения Субоператора, в отношении которого было направлено соответствующее уведомление, Контролер данных может в течение срока уведомления прекратить действие настоящего DPA в письменной форме. Если Контролер данных не прекращает свою деятельность в течение срока уведомления, это является свидетельством согласия Контролера данных на изменение Субоператора, в отношении которого было направлено соответствующее уведомление.

7.3 В любом случае, если Оператор данных использует услуги Субоператора, последний должен в рамках контракта выполнять те же обязательства, которые выполняет Оператор данных в отношении Обработки Персональных данных в соответствии с настоящим DPA.

8. ПРОЧИЕ ПОЛОЖЕНИЯ

8.1 Для вступления в силу изменений или дополнений к этому DPA, они должны оформляться в письменном виде. Несмотря на вышесказанное, Оператор данных может в любое время и без уведомления Контролера данных изменить технические, физические и организационные меры, изложенные в Приложении 2, при условии, что такое изменение не окажет существенного влияния на безопасность, конфиденциальность или целостность Персональных данных.

8.2. Ссылки в этом DPA на «письменный» или «в письменном виде» включают сообщения электронной почты и заказные письма.

8.3 Если какое-либо положение этого DPA станет недействительным, это не повлияет на действенность остальных условий. В случае признания какого-либо положения настоящего DPA недействительным, Стороны в любом случае будут стремиться добросовестно заменить признанное недействительным положение другим, имеющим исковую силу, действенным и законным, имеющим в максимально возможной степени правовое воздействие, равное или эквивалентное первоначальному положению.

8.4 Это DPA регулируется тем же действующим законодательством, что и ЛСКП.

ПРИЛОЖЕНИЕ 1 — СПЕЦИАЛЬНЫЕ УСЛОВИЯ ЮРИСДИКЦИИ

Если Контролер данных учрежден в одной из юрисдикций, перечисленных в Приложении 1, то к DPA применяются следующие условия, и такие условия имеют преимущественную силу в случае любого конфликта с другими положениями DPA. Все условия ЛСКП, которые не были специально изменены применимыми условиями для конкретной юрисдикции в этом Приложении, остаются неизменными и имеют полную силу.

Бразилия:
Стороны признают и соглашаются с тем, что должно применяться следующее изменение в DPA:

a) Все упоминания «Особых категорий Персональных данных» в DPA должны быть заменены на «Конфиденциальные персональные данные».

Мексика:
Стороны признают и соглашаются с тем, что должны применяться следующие изменения в DPA:

a) Все упоминания «Особых категорий Персональных данных» в DPA должны быть заменены на «Конфиденциальные персональные данные»;
b) Для применения Стандартных договорных положений все ссылки на «передачу» персональных данных должны толковаться как передача персональных данных в соответствии с мексиканским федеральным законом о защите персональных данных, находящихся в ведении частных лиц *(«Ley Federal de Protección de Datos Personales en Posesión de los Particulares*»).

Россия:
Помимо соблюдения положений DPA, Стороны обязуются выполнять следующее:

a) Настоящим Оператор данных подтверждает, что он полностью осознает, что целью деятельности по Обработке Персональных данных в соответствии с DPA является только предоставление Услуг по обработке, и будет обрабатывать Персональные данные только в тех целях, для которых Персональные данные были раскрыты, и Контролер данных требует этого от Оператора данных. Кроме того, по запросу Контролера данных Оператор данных должен незамедлительно подтвердить в письменной форме, что это правило соблюдается.
b) Перед раскрытием Персональных данных, полученных от граждан России, Оператору данных Контролер данных должен гарантировать, что все такие Персональные данные были записаны, систематизированы, накоплены, сохранены, уточнены (обновлены, изменены) и извлечены с использованием баз данных, расположенных на территории Российской Федерации, если такие Персональные данные были собраны любым способом, в том числе через Интернет.
c) Если Контролер данных обнаруживает незаконную обработку или неточность Персональных данных, Контролер данных должен немедленно дать указание Оператору данных заблокировать эти Персональные данные и инициировать проверку. Соответствующие Персональные данные должны быть заблокированы на весь период проверки. Если проверка подтверждает неточность Персональных данных, Контролер данных должен дать соответствующему Субъекту данных (его представителю) или органу по защите данных (если применимо) запрос на внесение поправок и направить их Оператору данных. Неточные Персональные данные должны быть изменены в ближайшее время, самое позднее в течение семи (7) рабочих дней со дня, когда изменения были переданы Оператору данных. Персональные данные будут разблокированы сразу после изменения.
d) Если обнаруживается, что Персональные данные обрабатываются незаконно, Контролер данных должен дать указание Оператору данных прекратить такую незаконную обработку в течение трех (3) рабочих дней с даты обнаружения. Если представляется невозможным устранить нарушения и обеспечить законность обработки Персональных данных, Контролер данных должен дать указание Оператору данных уничтожить незаконно обработанные Персональные данные в течение 10 (десяти) рабочих дней с даты обнаружения. Контролер данных также обязан уведомить соответствующего Субъекта данных (его представителя) и, если это требуется по закону, орган по защите данных об устранении нарушений.
e) Если Субъект данных отзывает свое согласие на обработку Персональных данных, Контролер данных должен немедленно уведомить об этом Оператора данных, а Оператор данных должен прекратить обработку и уничтожить Персональные данные этого Субъекта данных в течение тридцати (30) дней с даты о получении Контролером данных уведомления об аннулировании.

f) Если невозможно соблюсти сроки, указанные в пунктах d) и e) выше, Оператор данных должен заблокировать соответствующие Персональные данные по запросу Контролера данных на срок не более шести (6) месяцев и уничтожить эти Персональные данные в течение того же срока, если действующее законодательство не предписывает иное.

ЮАР:

Стороны признают и соглашаются с тем, что следующие изменения в DPA применяются в отношении определений, приведенных в разделе 1 DPA:

a) «Субъект данных» означает лицо, чьи Персональные данные обрабатываются.
b) «Персональные данные» означают личную информацию, как определено в POPIA, включая любую информацию, относящуюся к идентифицированному или идентифицируемому лицу.
c) «POPIA» означает Закон Южной Африки о защите личной информации 4 от 2013 года, а также любые обязательные правила, директивы, постановления, распоряжения или руководящие принципы, опубликованные в соответствии с POPIA.

США:

Помимо соблюдения положений DPA, Стороны обязуются выполнять следующее:

a) Каждая Сторона признает и соглашается, что сбор и раскрытие Персональных данных, переданных в Службы обработки, (i) не представляет собой намерение какой-либо из сторон, чтобы данная деятельность представляла собой продажу Персональных данных, и не является таковым намерением, а также (ii) если ценное вознаграждение, денежное или иное, предоставляется Авторизованным пользователем Оператору данных, такое ценное вознаграждение, денежное или иное, предоставляется за использование услуг по обработке, а не за раскрытие Персональных данных. Оператор данных не должен сохранять, использовать, раскрывать или продавать Персональные данные для каких-либо целей, кроме конкретной цели выполнения Услуг по обработке или иным образом, разрешенным законом или лицензионным соглашением. Во избежание сомнений Оператор данных не должен продавать Персональные данные или разрешать или иным образом позволять Субоператору делать то же самое, если иное не разрешено ЛСКП или применимым законодательством.

Приложение 2 — Меры безопасности, реализуемые Оператором данных

1. Контроль физического доступа в помещения и сооружения

Оператор данных будет реализовывать технические и организационные меры для контроля доступа к помещениям и объектам, в частности, для проверки авторизации для предотвращения несанкционированного доступа.

Конкретно:

- Система контроля доступа
- Считыватель удостоверений личности, магнитная карта, чип-карта
- Выдача ключей
- Дверные замки
- Сотрудники службы безопасности, охрана
- Средства наблюдения
- Система охранной сигнализации, видеонаблюдение/видеомониторинг

2. Контроль доступа к системам

Оператор данных должен реализовать технические (защита в виде идентификатора/пароля) и организационные меры для идентификации и аутентификации пользователей для предотвращения несанкционированного доступа к ИТ-системам.

Конкретно:

- Процедуры ввода пароля (включая специальные символы, минимальную длину, изменение пароля)
- Автоматическая блокировка (например, пароль или тайм-аут)
- Шифрование носителей данных, в том числе съемных и переносных.

3. Логический контроль доступа к данным

Оператор данных должен обеспечить предотвращение действий в ИТ-системах, на которые не распространяются выделенные права доступа, за счет использования основанного на требованиях определения схемы авторизации и прав доступа, а также мониторинга и регистрации доступа.

Конкретно:

- Права доступа на основе ролей (профили, роли, транзакции и объекты)
- Использование коммерческого решения для управления привилегированными учетными записями для облегчения безопасной аутентификации административных учетных записей в системах для обслуживания или других административных целей
- Автоматические отчеты, которые регулярно просматриваются и отслеживаются на предмет аномальной или подозрительной активности
- Доступ с использованием модели с минимальными привилегиями, чтобы разрешить доступ только к системам и (или) данным на основе служебной необходимости

4. Раскрытие и контроль защиты данных

Оператор данных будет контролировать раскрытие Персональных данных путем включения мер по транспортировке, пересылке и передаче или хранению данных на носителях данных (ручных или электронных) и для последующей проверки с помощью электронной передачи, пересылки данных и управления передачей.

Конкретно:

- Шифрование/туннелирование
- Электронная подпись
- Регистрация и постоянный мониторинг событий безопасности и предупреждений
- Транспортная безопасность для шифрования данных при передаче
- Шифрование данных в состоянии покоя
- Регулярная ротация ключей шифрования
- Ограничение доступа к ключам шифрования для ограниченных лиц
- Активация функции сложности пароля, с двухфакторной аутентификацией, необходимой для всех сеансов удаленного доступа

5. Система контроля входных данных

Оператор данных будет вести полную документацию об управлении данными и обслуживании, включая меры для последующей проверки того, были ли данные введены, изменены или удалены (убраны), и кем:

Конкретно:

- Системы регистрации и отчетности

6. Контроль работы

Оператор данных должен обрабатывать Персональные данные в соответствии с инструкциями Контролера данных и соглашается с мерами (техническими/организационными) для разделения ответственности между Контролером данных и Оператором данных: Конкретно:

- Однозначная формулировка договора
- Официальный ввод в эксплуатацию (форма запроса)
- Критерии выбора Оператора данных
- Мониторинг исполнения контрактов

7. Контроль доступности

Оператор данных гарантирует, что данные будут защищены от случайного или злонамеренного уничтожения или потери, принимая меры для обеспечения физической и логической безопасности данных.

Конкретно:

- Процедуры резервного копирования
- Зеркальное копирование жестких дисков, например, по технологии RAID
- Источник бесперебойного питания (ИБП)
- Удаленное или дисковое хранилище, которое реплицируется в альтернативные центры обработки данных
- Антивирусное программное обеспечение и (или) защита от вредоносных программ, которые регулярно обновляются, а также системы брандмауэров с поддержкой приложений, настроенные с использованием политики доступа «отказ по умолчанию», разрешающей только трафик, явно допустимый для бизнес-целей
- План обеспечения непрерывности бизнеса и аварийного восстановления

8. Контроль сегрегации

Оператор данных должен стремиться обеспечить, чтобы данные, собранные для различных целей, обрабатывались отдельно и не смешивались с другими данными клиентов, путем принятия конкретных мер для обеспечения раздельной Обработки (хранения, изменения, удаления, передачи) данных для различных целей:

Конкретно:

- Понятие «внутренний клиент»/ограничение использования
- Разделение функций (производство/тестирование)