УТВЕРЖДЕНО
приказом Индивидуального
предпринимателя Затолокиной Е.В.
от «01» сентября 2017 г.
№ 08-1/ПНА

ПОЛОЖЕНИЕ
о защите и обработке персональных данных клиентов

г. Калининград
2017 г.

Содержание

1. Общие положения

1.1 Положение о защите и обработке персональных данных клиентов (далее – Положение) определяет порядок обработки и защиты персональных данных клиентов Индивидуального предпринимателя Затолокиной Елены Валентиновны (далее – Оператор).

1.2 Положение разработано в соответствии со следующими нормативно-правовыми актами:

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

– Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

– Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119.

– Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21.

1.3 Положение предназначено для организации Оператором процесса обработки и защиты персональных данных клиентов согласно нормам и принципам действующего федерального законодательства.

1.4 Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению персональных данных, осуществляемых с использованием средств автоматизации и без их использования.

1.5 Настоящее Положение обязательно для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных клиентов.

2. Правовые основания и цели обработки персональных данных

2.1 Цель обработки персональных данных клиентов: оказание услуг, предусмотренных договором между Оператором и субъектом персональных данных.

2.2 Правовые основания обработки персональных данных клиентов:

– договор между Оператором и клиентом и (или);

– согласие клиентов на обработку персональных данных.

2.3 Обработка ПДн клиентов осуществляется на основе следующих принципов:

– обработка ПДн осуществляется на законной и справедливой основе;

– обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей;

– не допускается обработка ПДн, несовместимая с целями сбора ПДн;

– не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только ПДн, которые отвечают целям их обработки;

– содержание и объем обрабатываемых ПДн соответствует заявленным целям обработки;

– при обработке ПДн обеспечиваются их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн.

3. Перечень персональных данных

3.1 Категории сведений, являющихся персональными данными клиентов, обрабатываемых Оператором и подлежащих защите, содержатся в перечне персональных данных, утвержденном приказом руководителя Оператора

Состав персональных данных клиентов:

– фамилия, имя, отчество;

– дата рождения и место рождения;

– пол;

– гражданство;

– паспортные данные или данные иного удостоверяющего личность документа (серия, номер, дата выдачи, срок действия, код подразделения);

– адрес постоянной регистрации и проживания;

– контактный телефон;

– миграционная карта (серия, номер) (для иностранных граждан);

– виза (серия, номер, дата выдачи, срок действия, цель въезда) (для иностранных граждан).

3.2 Документы, содержащие персональные данные клиентов:

– анкета;

– уведомление о прибытии иностранного гражданина или лица без гражданства в место пребывания;

– регистрационная карта;

– копия документа, удостоверяющего личность (для иностранных граждан).

3.3 Сроки обработки персональных данных.

Обработка ПДн осуществляется с момента их получения Оператором и прекращается:

– по достижению целей обработки ПДн;

– в связи с отсутствием необходимости в достижении заранее заявленных целей обработки ПДн;

– в связи с отзывом согласия на обработку ПДн;

– в связи с ликвидацией Оператора как юридического лица.

Срок обработки ПДн клиентов – в течение срока действия договора, заключенного между Оператором и клиентом, и 3 года после его окончания, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

4. Конфиденциальность персональных данных

4.1 Оператор и иные лица, получившие доступ к персональным данным клиентов, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5. Технология обработки персональных данных

5.1 Клиент на рецепции вносит в регистрационную карту персональные данные, которые обрабатываются администратором, иностранные граждане также предоставляют документ, удостоверяющий личность. Персональные

данные из регистрационной карты вносятся в анкету и уведомление о прибытии иностранного гражданина или лица без гражданства в место пребывания. Данные хранятся в деревянном запираемом шкафу кабинета рецепции, а после передаются в архив.

5.2 Хранение персональных данных клиентов осуществляется в виде документов на бумажных носителях и в электронном виде (базы данных) на электронных носителях информации.

5.3 Хранение персональных данных клиентов на бумажных носителях в целях их защиты от несанкционированного доступа осуществляется согласно Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденному постановлением Правительства Российской Федерации 15 сентября 2008 г. № 687.

5.4 Обработка персональных данных клиентов, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных клиентов можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

5.5 Персональные данные клиентов в электронном виде хранятся в информационных базах данных на машинных носителях информации на сервере в серверном помещении.

5.6 При фиксации персональных данных клиентов на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. При обработке различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5.7 Материальные носители, содержащие персональные данные клиентов, должны храниться в сейфах, запираемых шкафах (ящиках) или запираемых помещениях.

5.8 За сохранность материальных носителей отвечает ответственные за хранение материальных носителей, утвержденные приказом руководителя Оператора.

5.9 Обработка персональных данных клиентов осуществляется работниками, имеющими доступ к персональным данным клиентов, на специально отведенных АРМ. Пользователь при работе с персональными данными клиентов на АРМ должен соблюдать требования Регламента по

обеспечению информационной безопасности персональных данных в информационных системах персональных данных, утвержденного Оператором.

5.10 Запрещается выносить документы, содержащие персональные данные клиентов, для работы с ними на дому, в гостинице и т.д. В необходимых случаях руководитель Оператора может в письменной форме разрешить исполнителям или другим работникам вынос из здания документов, содержащих персональные данные клиентов, для их согласования, подписи и т.п. в организации, находящиеся за пределами контролируемой зоны.

5.11 Командируемым работникам под их личную ответственность с письменного разрешения руководителя Оператора разрешается иметь при себе в пути следования документы, содержащие персональные данные клиентов.

5.12 О фактах утраты документов, содержащих персональные данные клиентов, дел и других материалов либо разглашения содержащихся в них сведений немедленно ставятся в известность руководитель Оператора. По факту утраты проводится служебное расследование и составляется акт, который представляется руководителю Оператора. Расследование проводится согласно Регламенту по расследованию инцидентов информационной безопасности в информационных системах персональных данных, утвержденного Оператором.

5.13 Черновики, документы, потерявшие актуальность, и испорченные экземпляры документов, содержащих персональные данные клиентов, не выбрасываются. По мере накопления таких материалов, работники, из числа имеющих доступ к персональным данным клиентов, уничтожают все накопившиеся черновые материалы способом, гарантирующим невозможность восстановления информации с уничтоженных документов. Уничтожение производится в соответствии с Инструкцией о порядке уничтожения персональных данных и оформляется актом.

5.14 Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиентов распространяются как на бумажные, так и на электронные носители информации.

6. Получение и передача персональных данных третьим лицам

6.1 Оператор в ходе своей деятельности имеет право получать от третьих лиц и передавать третьим лицам обрабатываемые персональные

данные в интересах и с согласия субъектов персональных данных, а также без согласия субъекта персональных данных - в случаях, предусмотренных федеральным законодательством.

7. Обязанности Оператора при сборе персональных данных клиентов

7.1 Правовой основой для начала обработки персональных данных клиентов является согласие клиента на обработку персональных данных. Типовая форма регистрационной карты содержащей согласие клиента на обработку его персональных данных приведена в Приложении №1а.

7.2 Персональные данные передаются третьей стороне только с согласия субъекта ПДн, перечень организаций и состав ПДн должен быть указан в согласии на обработку ПДн, если иное не установлено законодательством РФ. Типовая форма согласия клиента на передачу его персональных данных третьей стороне приведения в Приложении № 1б.

7.3 В случае поручения обработки персональных данных третей стороне в договоре между Оператором и третей стороной должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных». Типовая форма договора поручения представлена в Приложении №2а.

7.4 В случае передачи обработки персональных данных третьей стороне, с согласия субъекта ПДн, между Оператором и третьей стороной должно быть заключено соглашение о конфиденциальности. Типовая форма соглашение о конфиденциальности приведена в Приложении №2б.

7.5 Факт передачи материальных носителей, содержащих персональные данные клиентов, между Оператором и другими организациями оформляется актом приёма-передачи (Приложение №3).

7.6 В соответствии с п.1 ст. 22 ФЗ «О персональных данных» Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (в настоящее время - Роскомнадзор) об обработке персональных данных.

7.7 В случае наличия неполных сведений или изменения сведений, указанных в уведомлении, Оператор обязан уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор).

8. Права субъектов персональных данных

8.1 Субъекты персональных данных имеют право:

– знакомиться со сведениями, содержащими свои персональные данные, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

– выбирать представителей для защиты своих персональных данных;

– получать доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

– требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением федерального закона; при отказе Оператора исключить или исправить персональные данные субъект персональных данных имеет право заявить об этом в письменной форме;

– требовать от Оператора предоставления информации обо всех изменениях персональных данных, произведенных последним, а также уведомления всех лиц, которым по вине должностных лиц, были сообщены неверные или неполные персональные данные субъекта;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в суд любые неправомерные действия или бездействие Оператора при обработке его персональных данных.

8.2 При обращении субъекта персональных данных или его законного представителя по вопросам предоставления информации о персональных данных, относящихся к соответствующему субъекту, Оператор обязан сообщить данному субъекту информацию о наличии персональных данных, предоставить возможность ознакомления с ней.

8.3 Обращения субъектов персональных данных фиксируются в Журнале обращений субъекта персональных данных.

8.4 Порядок работы с обращениями субъектов персональных данных определен в Правилах рассмотрения запросов субъектов персональных данных, утвержденных Оператором.

9. Система допуска сотрудников к сведениям, составляющим персональные данные клиентов

9.1 Свободный доступ к персональным данным клиентов закрывается с целью их защиты. Лица, не имеющие доступа к персональным данным, применительно к ним относятся к категории посторонних.

9.2 Перечень лиц, имеющих право доступа к персональным данным клиентов для осуществления своих трудовых функций, устанавливается приказом руководителя Оператора.

9.3 Работники, в отношении которых руководителем Оператора было принято решение предоставить право доступа к персональным данным клиентов, допускаются к работе с ними только после принятия на себя следующих обязательств, отраженных в должностных инструкциях:

– нести персональную ответственность за сохранность доверенных им сведений, содержащих персональные данные клиентов;

– не допускать действий, способных повлечь утрату документов, содержащих персональные данные, разглашение или неправомерное искажение персональных данных;

– знать и неуклонно соблюдать требования локальных нормативных актов Оператора о режиме защиты персональных данных;

– незамедлительно сообщать своему непосредственному руководителю об утрате документов, содержащих персональные данные клиентов;

– давать письменные объяснения об известных им обстоятельствах при проведении разбирательств по фактам нарушения требований локальных нормативных актов Оператора о режиме защиты персональных данных, а также по фактам утраты и хищения документов, содержащих персональные данные;

– давать письменное обязательство о неразглашение сведений конфиденциального характера.

9.4 Работники, не принявшие указанные выше обязательства, к работе с персональными данными не допускаются.

9.5 Подписание работником обязательства о неразглашении сведений конфиденциального характера (приложение №4) является обязательным условием для его допуска к работе с персональными данными клиентов. Обязательство о неразглашении оформляется при устройстве на работу и хранится в личном деле работника. Контроль за своевременным подписанием обязательства о неразглашении сведений конфиденциального характера возлагается на ответственного за организацию обработки персональных данных.

9.6 Доступ к персональным данным клиентов предоставляется, только тем работникам, которым этот доступ необходим для выполнения служебных обязанностей, и в объёме, необходимом для качественного и своевременного выполнения порученных ему работ.

9.7 Список лиц, имеющих доступ к персональным данным, для каждой информационной системы персональных данных утверждается руководителем Оператора.

9.8 Перечень лиц, допущенных к работе в информационной системе персональных данных, поддерживается в актуальном состоянии. С этой целью проводятся следующие действия:

– Для каждой системы, на основании заявок от руководителей структурных подразделений, администратор информационной безопасности персональных данных в информационных системах персональных данных формирует перечень лиц, допущенных к обработке персональных данных для выполнения своих должностных обязанностей.

9.9 В случае, если сотрудник сторонней организации имеет доступ к персональным данным клиентов необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности персональных данных и обязанность сторонней организации и ее сотрудников по соблюдению требований законодательства в области защиты персональных данных.

9.10 Прекращение трудового договора, независимо от оснований, не освобождает работника от взятых обязательств о неразглашении сведений, составляющих персональные данные клиентов.

9.11 При устройстве на работу нового сотрудника, ответственный за обработку персональных данных знакомит под роспись в Журнале учета ознакомления работников, имеющих доступ к персональным данным, с организационно-распорядительными документами, регламентирующими защиту персональных данных, со следующими документами:

– Политика обработки и защиты персональных данных
– Положение об обработке и защите персональных данных работников
– Положение об обработке и защите персональных данных клиентов
– Приказ о допуске работников к персональным данным
– Приказ об утверждении перечня обрабатываемых персональных данных
– Регламент по обеспечению информационной безопасности персональных данных в информационных системах
– Инструкция о порядке учета, хранения, обращения и уничтожения съемных носителей, содержащих персональные данные

– Приказ об утверждении лиц, допущенных к персональным данным в информационной системе персональных данных

– Инструкция о порядке уничтожения персональных данных

– Инструкция о порядке доступа в помещения, где осуществляется обработка персональных данных.

– Правила осуществления внутреннего контроля информационной системы персональных данных

– Правила рассмотрения запросов субъектов персональных данных

– Регламент по расследованию инцидентов информационной безопасности.

9.12 Администратор информационной безопасности персональных данных в информационных системах персональных данных настраивает права учетной записи пользователя для доступа к персональным данным, обрабатываемых в информационной системе, вносит необходимые изменения в матрице доступа к информационной системе и вносит изменения в список лиц, допущенных к работе с персональными данными, который утверждается приказом руководителя Оператора.

9.13 Доступ третьих лиц к персональным данным разрешается только при наличии заявления запросившего их лица с указанием перечня необходимой информации, целей для которых она будет использована, с письменного согласия клиента, персональные данные которого затребованы.

9.14 Сообщение сведений о персональных данных субъекта его родственникам, членам семьи, иным близким ему людям также производится только при получении письменного согласия субъекта персональных данных.

9.15 При передаче персональных данных третьим лицам, в том числе представителям субъекта в порядке, установленном нормативными правовыми актами РФ и настоящим Положением, передаваемая информация ограничивается только теми персональными данными, которые необходимы для выполнения третьими лицами их функций.

9.16 Запрещается передача персональных данных в коммерческих целях без согласия субъекта персональных данных, а также иное использование персональных данных в неслужебных целях.

10. Обязанности работников Оператора, допущенных к персональным данным клиентов

10.1 Работники Оператора, допущенные к персональным данным клиентов **обязаны**:

– знать и выполнять требования организационно-распорядительных документов, регулирующих защиту и обработку персональных данных;

– хранить в тайне известные им персональные данные клиентов;

– информировать своего непосредственного руководителя и ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных о фактах нарушения порядка обращения с персональными данными клиентов, о попытках несанкционированного доступа к таким сведениям;

– строго соблюдать правила пользования документами и другими материальными носителями, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц;

– использоваться в работе только те документы, к которым получен доступ в силу исполнения прямых служебных обязанностей;

– о допущенных нарушениях установленного порядка работы, учета и хранения документов, а также о фактах разглашения, распространения персональных данных представлять письменные объяснения руководителю Оператора;

– убирать после окончания рабочего дня все съёмные носители и документы, содержащие персональные данные, в сейф или металлический шкаф.

10.2 Работникам **запрещается**:

– разглашать персональные данные клиентов;

– использовать персональные данные клиентов в личных интересах;

– выполнять на дому работы, связанные с персональными данными клиентов, без разрешения руководителя Оператора;

– выносить документы и другие носители информации, содержащие персональные данные клиентов, из здания Оператора без разрешения руководителя Оператора;

– использовать персональные данные клиентов в открытой переписке, статьях и выступлениях;

– снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для записи персональных данных без разрешения руководителя Оператора;

– передавать персональные данные клиентов по открытым каналам связи (Интернет);

– размещать на общедоступных сетевых ресурсах Оператора или в сети Интернет персональные данные клиентов;

– оставлять документы и другие материальные носители, содержащие персональные данные клиентов, без присмотра.

10.3 Приказом руководителя Оператора утверждаются Правила доступа в помещения, в которых осуществляется обработка персональных данных, список таких помещений и список лиц, имеющих доступ в эти помещения.

Лица, не имеющие доступ в помещение, где обрабатываются персональные данные клиентов, могут находиться там только в служебных целях и только в присутствие лиц, имеющих права допуска в данное помещение.

11. Условия обработки персональных данных, осуществляемой без использования средств автоматизации

11.1 Сотрудники, осуществляющие обработку персональных данных клиентов без использования средств автоматизации, должны быть проинформированы до начала обработки о категориях персональных данных, об особенностях и правилах обработки персональных данных, изложенных в настоящем Положении.

11.2 В типовых формах, в которые предполагается внесение персональных данных, должна содержаться следующая информация:

– цель обработки персональных данных, наименование и адрес Оператора, источник получения, срок обработки, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

– поле для проставления субъектом персональных данных отметки о согласии на обработку персональных данных без использования средств автоматизации.

11.3 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств

автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель

11.4 Носители персональных данных не должны оставаться без присмотра. Покидая рабочее место, лица, ответственные за хранение, должны убирать носители в запираемый шкаф или сейф.

12. Защита персональных данных клиентов

12.1 Оператор при обработке персональных данных клиентов принимает необходимые организационные и технические меры, в том числе использует шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

12.2 Руководители структурных подразделений несут ответственность за соблюдение режима конфиденциальности персональных данных и за сохранность материальных носителей, содержащих персональные данные, в своем структурном подразделении.

12.3 В целях обеспечения защиты персональных данных клиентов разрабатываются и утверждаются:

– списки лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения трудовых обязанностей;

– локальные нормативные акты и должностные инструкции;

– иные документы, регулирующие порядок обработки и обеспечения безопасности и конфиденциальности персональных данных.

12.4 Защита персональных данных клиентов от неправомерного их использования или утраты обеспечивается за счёт средств Оператора в порядке, установленном законодательством РФ.

12.5 В случае выявления неправомерных действий с персональными данными Оператор обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

12.6 Внутренняя защита персональных данных клиентов.

12.6.1 Персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом несгораемом шкафу или в запираемом металлическом сейфе.

12.6.2 Выдача ключей от сейфа производится руководителем структурного подразделения, в функции которого входит обработка определенных персональных данных (а на период его временного отсутствия - болезнь, отпуск и т.п. - лицом, исполняющим ее обязанности), только сотрудникам данного структурного подразделения. Сдача ключа осуществляется лично руководителю после закрытия сейфа или запираемого шкафа.

12.6.3 Персональные данные, содержащиеся на электронных носителях информации, хранятся в памяти персональных компьютеров пользователей. Доступ к указанным персональным компьютерам строго ограничен кругом лиц, ответственных за обработку персональных данных.

12.6.4 Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

– определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

– разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– внедрение и ввод в эксплуатацию системы защиты информации в соответствии с эксплуатационной и технической документацией;

– оценку эффективности принятых мер;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– анализ фактов несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание системы защиты персональных данных.

13. Правила работы с обезличенными персональными данными

13.1 Обезличивание персональных данных клиентов может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных Оператора и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

13.2 Способы обезличивания при условии дальнейшей обработки персональных данных:

– Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

– Для обезличивания персональных данных могут использоваться любые способы, не запрещенные законодательством.

13.3 Руководитель Оператора принимает решение о необходимости обезличивания персональных данных клиентов.

13.4 Порядок проведения обезличивания определен в Правилах работы с обезличенными персональными данными.

14. Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

14.1 Организация внутреннего контроля процесса обработки персональных данных клиентов осуществляется в целях изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

14.2 Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных клиентов направлены на решение следующих задач:

– Обеспечение соблюдения работниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих сферу персональных данных.

– Оценка компетентности работников, задействованных в обработке персональных данных.

– Обеспечение работоспособности и эффективности технических средств информационных систем защиты персональных данных и средств защиты персональных данных, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности персональных данных.

– Выявление нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений.

– Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки персональных данных, так и в работе технических средств информационной системы персональных данных.

– Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий.

– Осуществление контроля за исполнением рекомендаций и указаний по устранению нарушений.

14.3 Результаты контрольных мероприятий являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных, по модернизации технических средств информационных систем персональных данных и средств защиты персональных данных, по обучению и повышению компетентности работников, задействованных в обработке персональных данных.

14.4 Порядок проведение контроля регламентируется Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

15. Ответственность за разглашение персональных данных

15.1 Работники Оператора, обрабатывающие персональные данные клиентов, несут персональную ответственность за:

– не обеспечение конфиденциальности информации, содержащей персональные данные;

– неправомерный отказ субъекту персональных данных в предоставлении собранных в установленном порядке персональных данных либо предоставление неполной или заведомо ложной информации.

15.2 Ответственность за разглашение персональных данных клиентов.

15.2.1 Под распространением персональных данных понимаются преднамеренные или непреднамеренные действия, направленные на раскрытие персональных данных клиентов работниками Оператора неопределенному кругу лиц. Под предоставлением персональных данных понимаются действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

15.2.2 Ответственность за разглашение персональных данных клиентов несет персонально каждый работник Оператора, имеющий доступ к персональным данным и допустивший их несанкционированное распространение.

15.2.3 За разглашение персональных данных клиентов и нарушение порядка защиты таких данных работники Оператора, а также уволенные из него лица, привлекаются к ответственности в соответствии с законодательством Российской Федерации.

15.2.4 Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.