Утверждаю

Генеральный директор

ООО НКО «Тайдон»

_____ М.В. Наумова

«13» декабря 2022 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в ООО НКО «Тайдон»

г. Кемерово

Оглавление

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» с изменениями и Стандартом Банка России от 01.06.2014 г. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

1.2. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления, хранения и уничтожения документов, содержащих сведения, отнесенные к персональным данным (далее – ПДн) работников и клиентов (далее – субъекты ПДн) ООО НКО «Тайдон» (далее – Оператор), а также к ПДн, обрабатываемым в информационных системах персональных данных (далее - ИСПДн). Под работниками подразумеваются лица, заключившие трудовой договор.

1.3. В настоящем Положении используются термины в соответствии с их значениями, указанными в Федеральном законе от 27.07.2006 № 152-ФЗ.

1.4. Настоящее Положение разработано в целях обеспечения реализации требований законодательства РФ в области обработки ПДн, направленных на обеспечение защиты прав и свобод граждан при обработке их ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Цель настоящего Положения – защита ПДн работников и клиентов от несанкционированного доступа и разглашения; ПДн всегда являются конфиденциальной, строго охраняемой информацией.

1.5. Цели обработки ПДн

Сбор и обработка ПДн Оператором осуществляются исключительно в целях:

- обеспечения соблюдения актов законодательства и иных нормативно-правовых актов;
- заключения и исполнения договоров и соглашений в рамках трудовых, гражданско-правовых и иных отношений.

Оператор ПДн осуществляет обработку ПДн физических лиц в целях:

- осуществления кредитных операций, сделок, услуг и осуществления иной деятельности, предусмотренной действующим законодательством, в соответствии с выданной лицензией;
- предоставления информации, в том числе отчетности, надзорным и контрольным органам в соответствии с требованиями действующего законодательства;
- передачи ПДн или поручения их обработки третьим лицам в соответствии с действующим законодательством;
- формирования данных о кредитной истории;
- осуществления и исполнения функций, полномочий и обязанностей, возложенных на Оператора действующим законодательством, нормативно-правовыми и иными актами Банка России, федеральных органов исполнительной власти, уставом, лицензией и внутренними документами Оператора;
- заключения, исполнения и прекращения трудовых, гражданско-правовых и иных договоров и соглашений с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, рассмотрения возможности заключения трудового договора (соглашения), договора

гражданско-правового характера с субъектом ПДн (в порядке и в случаях, предусмотренных действующим законодательством и уставом Оператора);

- организации кадрового учета, обеспечения соблюдения актов законодательства и иных нормативно-правовых актов, содержащих нормы трудового права, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам;
- ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с действующим законодательством, а также уставом и внутренними документами Оператора;

1.6. Принципы, условия и сроки обработки ПДн

Обработка ПДн осуществляется на основе следующих принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн конкретным, заранее определенным и заявленным при сборе ПДн законным целям, а также полномочиям Оператора;
- соответствия содержания, объема и характера обрабатываемых ПДн, способов обработки ПДн заявленным целям обработки ПДн;
- достаточности обрабатываемых ПДн для целей их обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- достоверности ПДн, их точности и актуальности по отношению к целям их обработки, принятия Оператором необходимых мер (обеспечения их принятия) по удалению или уточнению неполных или неточных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн (баз данных, содержащих ПДн).

Обработка ПДн осуществляется на основании условий, определенных законодательством. Получение и обработка ПДн в случаях, предусмотренных Законом N 152-ФЗ, осуществляется с письменного согласия субъекта ПДн. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, по собственной воле и в своих интересах.

Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Оператором.

Согласие на обработку ПДн может быть отозвано субъектом ПДн в установленном порядке. В случае отзыва субъектом ПДн согласия на обработку ПДн Оператор прекращает обработку указанных ПДн в порядке, установленном законодательством.

Оператор вправе обрабатывать ПДн (продолжить обработку ПДн) без согласия субъекта ПДн при наличии оснований, предусмотренных законодательством (пункты 2 - 11 части 1 статьи 6, часть 2 статьи 10 и часть 2 статьи 11 Закона N 152-ФЗ).

Оператор не осуществляет обработку специальных категорий ПДн (ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни).

Обработка сведений о состоянии здоровья субъекта ПДн осуществляется в соответствии с действующим законодательством (ТК РФ, Федеральным законом "Об обязательном медицинском страховании в Российской Федерации", пунктом 2.3 части 2 статьи 10 Закона N 152-ФЗ).

Обработка биометрических ПДн (сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность) Оператором не осуществляется.

Хранение полученных Оператором ПДн осуществляется на материальных (бумажных и электронных) носителях (в том числе в ИСПДн). Право доступа к ПДн на материальных носителях субъектов ПДн имеют (получают) только те работники Оператора, которым это необходимо для выполнения их должностных обязанностей и которые в законном порядке наделены соответствующими полномочиями и правами доступа к ПДн и средствам их обработки. Доступ иных лиц к ПДн, обрабатываемым Операторaом, может быть предоставлен исключительно в предусмотренных законодательством случаях и в установленном законом порядке.

Передача ПДн субъектов ПДн третьим лицам осуществляется Оператором в соответствии с требованиями действующего законодательства. Оператор не вправе передавать ПДн третьей стороне без согласия субъекта, за исключением случаев, предусмотренных законодательством РФ. При передаче ПДн Оператор должен предупредить лиц, получающих ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило, было (будет) соблюдено. Оператор вправе поручить обработку ПДн третьей стороне с согласия субъекта ПДн и в иных случаях, предусмотренных действующим законодательством, на основании заключаемого с этой стороной договора (далее - поручение). Третья сторона, осуществляющая обработку ПДн по поручению Оператора, обязана соблюдать принципы и правила обработки ПДн, предусмотренные Законом N 152-ФЗ, обеспечивая конфиденциальность и безопасность ПДн при их обработке.

ПДн относятся к охраняемой информации, доступ к которой ограничивается в соответствии с законодательством РФ, кроме случаев обезличивания (когда невозможно определить принадлежность ПДн к конкретному субъекту) и общедоступности (когда доступ к ПДн предоставлен с согласия субъекта ПДн неограниченному кругу лиц).

Доступ работникам Оператора к ПДн, подлежащим обработке, предоставляется в соответствии со Списком работников, доступ которых к ПДн, обрабатываемым в ИСПДн, в том числе без использования средств автоматизации, необходим для выполнения служебных обязанностей, утверждаемым приказом генерального директора (Приложение 1). При уходе в отпуск, направлении в служебную командировку и в иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные материальные носители, содержащие ПДн клиентов и (или) работников Оператора, лицу, на которое приказом будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, документы и иные носители, содержащие указанные ПДн, передаются другому работнику, имеющему доступ к таким ПДн, по указанию руководителя структурного подразделения.

Оператора за свой счет обеспечивает необходимые правовые, организационные и технические меры для обеспечения безопасности и защиты ПДн от неправомерного (несанкционированного) или случайного доступа к ним, уничтожения, изменения,

блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

Сроки обработки и хранения ПДн у Оператора определяются в соответствии со сроком действия договора (гражданско-правовых отношений) с субъектом ПДн, сроками хранения документов, содержащих ПДн (на бумажных и электронных носителях), установленными Приказом Росархива от 20.12.2019 N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», сроком исковой давности, в соответствии с иными требованиями, определяющими сроки обработки и хранения ПДн, установленными актами законодательства и иными нормативно-правовыми актами, а также сроком действия согласия субъекта на обработку его ПДн.

Условиями для прекращения обработки ПДн могут быть:

- достижение целей обработки ПДн;
- истечение срока действия согласия на обработку ПДн;
- отзыв субъектом согласия ПДн на обработку его ПДн;
- выявление неправомерной обработки ПДн.

Хранение ПДн осуществляется в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Все используемые Оператором базы данных, содержащие ПДн граждан РФ, находятся на территории РФ. Трансграничная передача ПДн не используется.

1.7. Настоящее Положение и изменения к нему утверждаются генеральным директором. Все субъекты ПДн ознакамливаются под роспись с данным Положением и изменениями к нему. В случае сбора ПДн с использованием информационно-телекоммуникационных сетей, Оператор опубликовывает настоящее Положение в соответствующей информационно-телекоммуникационной сети, а также обеспечивает доступ к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети

2. Объем и категории обрабатываемых ПДн, категории субъектов ПДн, источники ПДн.

Согласно Федеральному закону от 27.07.2006 №152- ФЗ «О персональных данных»:

- **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
- **персональные данные, разрешенные субъектом персональных данных для распространения**, - ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн путем дачи согласия на обработку ПДн, разрешенных субъектом ПДн для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 г. № 152- ФЗ.

Содержание и объем обрабатываемых ПДн должны соответствовать заявленным в настоящем Положении целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

К субъектам ПДн, обрабатываемых Оператором, относятся:

- физические лица, состоящие (состоявшие) с Оператором в договорных и иных гражданско-правовых отношениях, кандидаты на замещение вакантных должностей, а также родственники работников;
- физические лица, обратившиеся к Оператору с целью получения информации или заключения договора;
- иные физические лица, чьи ПДн обрабатываются Оператором в соответствии с требованиями законодательства РФ;
- физические лица - представители, правопреемники, выгодоприобретатели, бенефициарные владельцы вышеперечисленных лиц.

В зависимости от субъекта ПДн Оператор обрабатывает ПДн следующих категорий субъектов ПДн:

- ПДн работника (информация, необходимая Операторау в связи с трудовыми или гражданско-правовыми отношениями и касающаяся конкретного работника), кандидата на замещение вакантной должности, родственников работника;
- ПДн аффилированного лица, инсайдера или ПДн руководителя, участника (акционера) или работника (сотрудника) юридического лица, являющегося аффилированным лицом по отношению к Оператору (информация, необходимая Оператору для отражения в отчетных документах о деятельности Оператора в соответствии с требованиями федеральных законов, нормативных документов Банка России и иных нормативно-правовых актов);
- ПДн клиента, а также ПДн руководителя, участника (акционера) или работника (сотрудника) юридического лица, являющегося клиентом Оператора (информация, необходимая Оператору для выполнения своих обязательств в рамках договорных отношений с клиентом и для выполнения требований законодательства РФ);
- ПДн потенциального клиента, контрагента, партнера, а также ПДн руководителя, участника (акционера) или работника (сотрудника) юридического лица, являющегося потенциальным клиентом, партнером, контрагентом (информация, необходимая Оператору в целях рассмотрения вопроса о заключении договорных отношений (проведении операций и сделок с потенциальным клиентом, контрагентом, партнером) и для выполнения требований законодательства РФ);
- ПДн заемщика (залогодателя, поручителя, принципала) (потенциального заемщика (залогодателя, поручителя, принципала)), а также ПДн руководителя, участника (акционера) или сотрудника юридического лица, являющегося заемщиком (залогодателем, поручителем, принципалом) (потенциальным заемщиком (залогодателем, поручителем, принципалом)) (информация, необходимая Оператору для выполнения (оценки выполнения) своих договорных обязательств и осуществления прав в рамках соответствующего договора, заключенного с заемщиком (залогодателем, поручителем, принципалом) (предполагаемого к заключению с потенциальным заемщиком (залогодателем, поручителем, принципалом))), в целях минимизации рисков, связанных с нарушением обязательств по кредитному договору (договору залога, договору поручительства, договору о предоставлении гарантии) и для выполнения требований законодательства РФ;

- ПДн представителя (информация, необходимая Оператору для выполнения своих обязательств в рамках договорных и иных отношений с представляемым лицом и для выполнения требований законодательства РФ);
- ПДн выгодоприобретателя (физического лица), бенефициарного владельца (информация, необходимая Оператору для выполнения требований законодательства РФ).

ПДн субъектов ПДн, не состоящих в трудовых или гражданско-правовых отношениях или иных договорных отношениях с Оператором, проходящих на территорию (в помещения), на которой находится Оператор, а также иных субъектов, чьи ПДн обрабатываются Оператором в соответствии с требованиями законодательства.

Оператор рассматривает следующие категории ПДн, которые в зависимости от категории субъекта ПДн могут обрабатываться или не подлежат обработке:

- **ПДн общей категории** - общедоступные ПДн, к данной категории относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн) (фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту ПДн). Оператором осуществляется обработка ПДн этой категории в отношении всех категорий субъектов ПДн;
- **ПДн специальной категории** - к данной категории относятся ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта ПДн, а также иные ПДн, относимые действующим законодательством к специальным категориям ПДн. Обработка специальных категорий ПДн Оператором не осуществляется, за исключением случаев, предусмотренных законодательством;
- **Биометрические ПДн** – обработка ПДн этой категории Оператором не осуществляется, за исключением случаев, предусмотренных законодательством.

Источники ПДн работника:

- анкета;
- автобиография;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- трудовой договор;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;

- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к Пдн работника;
- рекомендации, характеристики и т.п.

Источники Пдн клиентов:

- Кредитная заявка.
- Анкета.
- Паспорт или иные документы, удостоверяющие личность и их копии.
- Свидетельства о постановке на учет в налоговом органе и его копия.
- Справка с места работы о доходах физического лица не менее чем за последние шесть месяцев, либо за фактически отработанное время (заверенная надлежащим образом).
- Иные документы, подтверждающие доходы физического лица.
- Справка с работы о доходах иных родственников (при рассмотрении совокупного дохода) не менее чем за последние шесть месяцев, либо за фактически отработанное время (заверенная надлежащим образом).
- Иные документы, подтверждающие доходы иных родственников (при рассмотрении совокупного дохода).
- Документы, подтверждающие право собственности на предмет залога и их копии;
- Документы, подтверждающие право собственности на недвижимое/движимое имущество и их копии.

Источники ПДн поручителей:

- Паспорт или иные документы, удостоверяющие личность и их копии.
- Анкета.
- Справка с места работы о доходах поручителя не менее чем за последние шесть месяцев, либо за фактически отработанное время (заверенная надлежащим образом).
- Иные документы, подтверждающие доходы поручителя.

Оператором создаются и хранятся следующие документы, содержащие данные о субъектах ПДн:

- анкета клиента - физического лица, клиента - юридического лица (с данными об учредителях, директорах);
- ходатайство на пролонгацию кредита заемщика — физического лица;
- заявление на открытие счета;
- кредитный договор;
- кассовые документы, содержащие ПДн клиентов;
- копии документов, удостоверяющих личность, а также иных документов, предоставляемых субъектами ПДн, и содержащих ПДн;
- свидетельство о государственной регистрации в качестве индивидуального предпринимателя (оригинал или копия, заверенная надлежащим образом);
- трудовые книжки;
- анкета работника – субъекта ПДн;
- заявления работника – субъекта ПДн.

3. Права и обязанности оператора ПДн

3.1. Оператор ПДн имеет право:

- осуществлять проверку точности, достоверности и актуальности предоставляемых ПДн в случаях, объеме и порядке, предусмотренных и установленных законодательством;
- отказывать в предоставлении ПДн в случаях, предусмотренных законодательством;
- предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством;
- использовать ПДн субъекта без его согласия в случаях, предусмотренных законодательством;
- отказать субъекту ПДн в случае его отказа от предоставления (непредставления) Оператору своих ПДн, обработка которых необходима для предоставления субъекту продуктов и услуг, в предоставлении соответствующих продуктов и услуг в законном порядке, за исключением случаев, предусмотренных законодательством;
- отстаивать свои интересы в суде;
- реализовывать иные права, предусмотренные законом или договором.

3.2. Оператор ПДн обязан:

- не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн и если иное не предусмотрено законодательством;
- использовать ПДн субъекта без его согласия в случаях, предусмотренных законодательством;
- не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством;
- предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговым, правоохранительным органам и др.);
- по требованию субъекта ПДн прекратить обработку его ПДн, за исключением случаев, предусмотренных законодательством;
- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом N 152-ФЗ и иными законодательными актами РФ;
- все ПДн работника следует получать у него самого. Если ПДн работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа работника дать письменное согласие на их получение;
- работодатель не имеет права получать и обрабатывать ПДн работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;
- работодатель не имеет права получать и обрабатывать ПДн работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
- в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, Оператор обязан с момента выявления такого инцидента, уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Оператором на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).
- в случае достижения цели обработки ПДн Оператор обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.
- в случае отзыва субъектом ПДн согласия на обработку его ПДн Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей их обработки, уничтожить ПДн или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами
- в случае обращения субъекта персональных данных к Оператору с требованием о прекращении обработки ПДн Оператор обязан в срок, не превышающий десяти рабочих дней с даты получения Оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку ПДн). Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
- В случае отсутствия возможности уничтожения ПДн в течение указанного срока Оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

- уведомить Роскомнадзор о начале или осуществлении любой обработки ПДн за исключением случаев, когда ПДн обрабатываются исключительно без средств автоматизации.

4. Права и обязанности субъекта ПДн

4.1. Субъект ПДн (его представитель) имеет право:

- свободного бесплатного доступа к своим ПДн, включая право на получение копий любой записи, содержащей ПДн, за исключением случаев, предусмотренных законодательством;
- требовать уточнения (изменения) своих ПДн (ПДн субъекта), их блокирования или уничтожения, в случае если ПДн являются неполными, неточными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав (прав субъекта ПДн);
- требовать предоставления перечня своих ПДн (ПДн субъекта), обрабатываемых Оператором, и информации об источнике их получения, если иное не предусмотрено законодательством;
- получать информацию о сроках обработки своих ПДн (ПДн субъекта), в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные (неточные, неактуальные) его ПДн (ПДн субъекта), обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке неправомерные действия или бездействие Оператора при обработке его ПДн (субъекта ПДн);
- на защиту своих прав (прав субъекта ПДн) и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- определять своих представителей для защиты своих ПДн;
- отозвать согласие на обработку своих ПДн (ПДн субъекта), за исключением случаев, предусмотренных законодательством;
- реализовывать иные права, предусмотренные законом или договором.

4.2. Субъект ПДн (его представитель) обязан:

- своевременно предоставлять Оператору сведения об изменении своих ПДн (ПДн субъекта), если такая обязанность предусмотрена договором между субъектом ПДн и Оператором, законодательством или внутренними документами Оператора;
- при предоставлении Оператору своих ПДн (ПДн субъекта) обеспечивать на момент предоставления ПДн их точность, достоверность и актуальность, за которые субъект несет ответственность в соответствии с действующим законодательством;
- выполнять иные обязанности, предусмотренные законом или договором.

4.3. Обращения субъектов ПДн ведется в журнале учета обращений граждан (Приложение 2).

5. Сбор, обработка, хранение и уничтожение ПДн

5.1. Обработка ПДН - это получение, хранение, комбинирование, передача или любое другое использование ПДн субъекта ПДн.

5.2. Целью обработки ПДн является:

- осуществление возложенных на Оператора законодательством Российской Федерации функций, в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», нормативными актами Банка России, а также другими нормативными актами РФ, Уставом и нормативными актами Оператора;
- организация учета служащих Оператора для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия служащему в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и внутренними актами Оператора.

5.3. Все ПДн субъекта ПДн следует получать у него самого, заручившись его письменным согласием на обработку и использование ПДн. Если ПДн работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

5.4. Оператор должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДН и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

5.5. Субъект ПДн предоставляет Оператору достоверные сведения о себе. Оператор проверяет достоверность сведений, сверяя данные, предоставленные субъектом ПДн, с имеющимися Оператора документами. Предоставление субъектом ПДн – работником Оператора подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора. Предоставление субъектом ПДн – клиентом Оператора или его поручителем подложных документов или ложных сведений при заключении договора кредитования является основанием для запуска процедуры расторжения кредитного договора или договора поручительства.

5.6. Согласия на обработку ПДН работников (Приложение 5), согласие на распространение ПДн (Приложение 6) хранятся в их личных делах.

5.7. Получение согласия близких родственников работника на обработку их ПДн не требуется при заполнении анкет в объеме, предусмотренном унифицированной формой N Т-2.

5.8. При поступлении на работу работник заполняет анкету и автобиографию.

Анкета представляет собой перечень вопросов о ПДн работника. Анкета заполняется работником самостоятельно. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркиваний, прочерков, помарок в строгом соответствии с записями, которые содержатся в его личных документах.

Автобиография - документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности принимаемого

работника. Автобиография составляется в произвольной форме, без помарок и исправлений.

Анкета и автобиография работника хранятся в личном деле работника. В личном деле также хранятся иные документы персонального учета, относящиеся к ПДн работника.

Личное дело работника оформляется после издания приказа о приеме на работу. Все документы личного дела подшиваются в обложку образца, установленного Оператором. На ней указываются фамилия, имя, отчество работника, номер личного дела. К каждому личному делу прилагаются две фотографии работника размером 3х4 сантиметра.

Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются.

Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных,

Сроки хранения ПДн субъектов, относящихся к кредитным правоотношениям, составляют 10 лет (ст. 7 ФЗ № 218 "О кредитных историях").

Сроки хранения ПДн субъектов, относящихся к трудовым правоотношениям, составляют 50 лет. («Приказ Росархива от 20.12.2019 N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения».)

Сроки хранения личных дел (заявления, автобиографии, копии приказов и выписки из них, копии личных документов, характеристики, листки по учету кадров, анкеты и др.) руководства Оператора, членов контрольных органов, а также работников, имеющих государственные и иные звания, премии, награды, ученые степени и звания - постоянно.

Документы (анкеты, автобиографии, листки по учету кадров, заявления, рекомендательные письма, резюме и др.) лиц, не принятых на работу хранятся 1 год.

Сроки хранения ПДн субъектов, относящихся к доходам субъектов, составляют 5 лет (Статья 23 НК РФ).

Сроки хранения гражданско-правовых договоров, содержащих ПДн субъектов, а также сопутствующих документов – 50 лет с момента окончания действия договоров (Приказ Росархива от 20.12.2019 N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения").

В течение срока хранения ПДн не могут быть обезличены или уничтожены. По истечении срока хранения ПДн подлежат уничтожению либо обезличиванию.

Уничтожение ПДн на бумажных носителях осуществляется по истечении срока хранения ПДн путем сожжения с составлением акта об уничтожении ПДн. На электронных носителях уничтожение ПДн осуществляется путем удаления из баз данных, а также путем размагничивания носителя.

6. ПЕРЕДАЧА ПДн

При передаче ПДн субъекта ПДн Оператор должен соблюдать следующие требования:

- не сообщать ПДн третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральным законом;
- не сообщать ПДн субъекта ПДн в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих ПДн субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн субъекта ПДн, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен ПДн субъектов ПДн в порядке, установленном федеральными законами;
- разрешать доступ к ПДн субъекта ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн субъекта ПДн, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника - субъекта ПДн, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать ПДн работника представителям работников в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми ПДн работника, которые необходимы для выполнения указанными представителями их функций;
- установленные работником запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) ПДн, разрешенных для распространения, не действуют в случаях обработки ПДн в государственных, общественных и иных публичных интересах, определенных законодательством РФ;
- ПДн субъекта ПДн могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

7. ДОСТУП К ПДн

7.1. Право внутреннего доступа к ПДн сотрудника Оператора имеют:

- генеральный директор;
- секретарь-референт (ответственный за ведение и учет кадров);
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения) по согласованию с генеральным директором;
- при переводе из одного структурного подразделения в другое доступ к ПДн сотрудника может иметь руководитель нового подразделения по согласованию с генеральным директором;
- сотрудники бухгалтерии (главный бухгалтер, заместитель главного бухгалтера, заведующий кассой);
- сам работник, носитель данных.

7.2. Внешний доступ. ПДн сотрудника Оператора могут представляться в следующие государственные и негосударственные функциональные структуры и с соблюдением порядка, установленного законодательством:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;

- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

7.3. Предоставление сведений другим организациям. Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только на основании письменного запроса на бланке организации с приложением копии заявления работника.

7.4. ПДн работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

7.5. Право доступа к ПДн субъекта ПДн – клиента или поручителя имеют:

- генеральный директор;
- сотрудники отдела по работе с клиентами;
- сотрудники бухгалтерии - к тем данным, которые необходимы для выполнения сотрудниками бухгалтерии обязанностей, предусмотренных должностными инструкциями;
- сотрудники службы внутреннего контроля;
- сотрудники юридического отдела;
- другие сотрудники Оператора для выполнения ими их функциональных обязанностей;

7.6. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые Оператором способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Оператором обязанностей;
- иные сведения, предусмотренные федеральными законами.

Сведения предоставляются субъекту ПДН или его представителю Оператором в течение десяти рабочих дней с момента обращения либо получения Оператором запроса субъекта ПДн или его представителя.

7.7. Внешний доступ. ПДн клиентов Оператора и их поручителей вне Оператора могут представляться в следующие государственные и негосударственные функциональные структуры и с соблюдением порядка, установленного законодательством:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- Бюро кредитных историй.

7.8. Работники Оператора, получившие доступ к ПДн субъекта, обязаны использовать их лишь в целях, для которых сообщены ПДн и обязаны соблюдать режим секретности (конфиденциальности) обработки и использования полученной информации (ПДН субъектов).

8. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДн

8.1. Организация и проведение мероприятий по обеспечению безопасности и защиты ПДн осуществляются Оператором в соответствии с настоящей Положением и иными внутренними документами Оператора.

8.2. В целях обеспечения безопасности и защиты ПДн при их обработке Оператор принимает необходимые и достаточные правовые, организационные и технические меры (или обеспечивает их принятие) для защиты ПДн от неправомерного (несанкционированного) или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Указанные меры осуществляются Оператором в строгом соответствии с требованиями законодательства, нормативно-правовых и иных актов в области обработки и защиты ПДн.

8.3. В состав и перечень необходимых и достаточных для обеспечения выполнения требований законодательства мер, принимаемых Оператором и направленных на обеспечение безопасности и защиты ПДн, которые в соответствии со статьей 18.1 Закона N 152-ФЗ определяются Оператором самостоятельно, входят:

8.3.1. Правовые меры:

- обязательство работника Оператора, закрепленное в трудовом договоре, заключенном между Оператором и работником, о неразглашении конфиденциальной информации;
- обязанность работников Оператора, закрепленная во внутренних документах Оператора, выполнять требования по соблюдению конфиденциальности и защиты ПДн работников и клиентов Оператора, ставших известными работнику в рамках исполнения им своих должностных обязанностей;
- обязательное включение в заключаемые Оператором с взаимодействующими организациями и физическими лицами соглашения о передаче ПДн требований соблюдения конфиденциальности (включая обязательство неразглашения) и обеспечения безопасности ПДн при их обработке;
- документальное оформление требований к безопасности обрабатываемых данных.

8.3.2. Организационные меры:

- назначение должностного лица Оператором, ответственного за организацию работ по защите ПДн;
- разработка и внедрение внутренних документов по вопросам обработки и защиты ПДн, а также внутренних документов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений установленных процедур по обработке ПДн и устранение последствий таких нарушений;
- установление персональной ответственности работников Оператора за обеспечение безопасности обрабатываемых ПДн;
- ознакомление работников Оператора, непосредственно осуществляющих обработку ПДн, с требованиями и содержанием актов законодательства, нормативно-правовых и иных актов Банка России, федеральных органов исполнительной власти, настоящей политикой и иными внутренними документами Оператора в области обработки ПДн, обеспечения их безопасности и защиты;
- мониторинг изменений законодательства, нормативно-правовых и иных актов в сфере обработки и защиты ПДн, ознакомление со значимыми изменениями и указанными рекомендациями всех работников Оператора, непосредственно осуществляющих обработку ПДн, и приведение в соответствие с ними внутренних документов Оператора (в том числе регламентов, инструкций и т.д.);
- контроль выполнения подразделениями, должностными лицами и работниками Оператора требований законодательства, нормативно-правовых актов, настоящей политики и иных внутренних документов Оператора в области обработки и защиты ПДн, контроль соответствия обработки и защиты ПДн указанным требованиям;
- классификация ПДн, ИСПДн (согласно требованиям законодательства);
- реализация принципа достаточности обрабатываемых ПДн (при определении состава обрабатываемых ПДн субъектов ПДн, Оператор руководствуется минимально необходимым составом ПДн для достижения целей получения и обработки ПДн);
- своевременное выявление угроз безопасности ПДн (в том числе при их обработке в ИСПДн), разработка и утверждение моделей угроз безопасности ПДн в соответствии с требованиями законодательства;
- учет машинных носителей ПДн;
- хранение материальных носителей ПДн в закрытых шкафах, ящиках, сейфах;
- организация контроля доступа в помещения и здания Оператора, их охрана в рабочее и нерабочее время, ограничение доступа в помещения, где хранятся ПДн;
- содержание специалистов по защите информации, организация системы их профессиональной подготовки;
- организация и реализация системы ограничения (разграничения) доступа пользователей (обслуживающего персонала) к документам, информационным ресурсам и машинным носителям информации, информационным системам и связанным с их использованием работам;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- систематический анализ (мониторинг) безопасности ПДн, регулярные проверки и совершенствование системы их защиты;
- контроль и оценка эффективности принимаемых мер по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

8.3.3. Технические меры:

- организационно-технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимые для выполнения требований к защите ПДн, исполнение которых обеспечивают установленные Правительством РФ уровни защищенности ПДн;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер по недопущению подобных инцидентов в дальнейшем;
- применение программных средств защиты информации при обработке ПДн, в т. ч. в ИСПДн (идентификация и проверка подлинности субъектов доступа по паролю условно-постоянного действия не менее шести буквенно-цифровых символов, антивирусная защита, межсетевое экранирование при подключении к Интернету, резервное копирование информации и ее восстановление после сбоев и т.д.);
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- иные технические меры, разрабатываемые и принимаемые Оператором в соответствии с требованиями законодательства, включая нормативные акты и требования уполномоченных органов.

8.4. С учетом важности и необходимости обеспечения безопасности ПДн Оператор постоянно совершенствует системы защиты ПДн, обрабатываемых в рамках выполнения основной деятельности Оператора, принимает дополнительные меры, направленные на защиту информации о клиентах, работниках, контрагентах и других субъектах ПДн. В целях повышения эффективности указанных систем и мер Оператор руководствуется рекомендациями надзорных и контрольных органов, а также лучшими российскими и международными практиками.

9. КРИТЕРИИ И ПОРЯДОК ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИСПДн

9.1. В ООО НКО «Тайдон» проведена классификация ИСПДн, утвержденная «Актом классификации ИСПДн».

9.2. Классификация ИСПДн проводится начальником отдела автоматизации совместно с ответственным сотрудником по информационной безопасности и согласовывается с генеральным директором. На основании анализа ИСПДн составляется список ИСПДн и акт классификации ИСПДн. (Приложение 3 и 4 соответственно).

9.3. Пересмотр списка ИСПДн и акта классификации ИСПДн проводится 1 раз в год.

9.3.1. Все ИСПДн относятся к информационным системам, обрабатывающим иные категории ПДн, в соответствии с пунктом 5 Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

9.3.2. Критериями классификации ИСПДн являются основные классы ИСПДн:

- ИСПДн обработки специальных категорий персональных данных - **ИСПДн-С** (В соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ "О персональных данных" к специальным категориям персональных данных относятся персональные данные, касающиеся расовой, национальной

принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.)

- ИСПДн обработки биометрических персональных данных - **ИСПДн-Б** (В соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ "О персональных данных" к биометрическим персональным данным относятся сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность);
- ИСПДн обработки общедоступных персональных данных - **ИСПДн-Д** (В соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ "О персональных данных" к общедоступным персональным данным относятся персональные данные, полученные из общедоступных источников персональных данных, включенных туда с письменного согласия субъекта персональных данных).
- ИСПДн обработки персональных данных, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным - **ИСПДн-И**;

9.4. На основе Отраслевой модели угроз безопасности персональных данных при их обработке в информационных системах ПДн Оператором определен и документально зафиксирован «Стандарт Моделей угроз и нарушителей информационной безопасности при обработке персональных данных ООО НКО «Тайдон»

10. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДн В ИСПДн

10.1. Требования по обеспечению безопасности ПДн в ИСПДн в ООО НКО "Тайдон" реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации. Реализация требований по обеспечению безопасности ПДн осуществляется по согласованию и под контролем ответственного сотрудника по ИБ.

10.2. Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн осуществляются по согласованию и под контролем ответственного сотрудника по информационной безопасности.

10.3. Все информационные активы, принадлежащие ИСПДн, должны быть защищены от воздействий вредоносного кода, а так же определены и документально зафиксированы требования по обеспечению безопасности ПДн средствами антивирусной защиты.

10.4. Определяется система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн.

10.5. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений обеспечивают безопасность ПДн при их обработке в ИСПДн. Работники, осуществляющие обработку ПДн в ИСПДн, действуют строго в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдать требования документов по обеспечению ИБ.

10.6. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению ИБ ИСПДн, возлагаются приказами на администраторов информационной безопасности ИСПДн.

10.7. Порядок действий администратора информационной безопасности ИСПДн и персонала, занятых в процессе обработки ПДнх, определен инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн.

Указанные инструкции (руководства):

- устанавливают требования к квалификации администратора информационной безопасности и персонала в области защиты информации, а также актуальный перечень защищаемых объектов и правила его обновления;
- содержат в полном объеме актуальные (по времени) данные о полномочиях пользователей;
- содержат данные о технологии обработки информации в объеме, необходимом для администратора информационной безопасности;
- устанавливают порядок и периодичность анализа журналов регистрации событий (архивов журналов);
- регламентируют другие действия администратора информационной безопасности и персонала, предусмотренные настоящими рекомендациями.

Параметры конфигурации средств защиты и механизмов защиты информации от НСД, используемых в зоне ответственности администратора информационной безопасности, определяются в эксплуатационной документации на ИСПДн. Порядок и периодичность проверок установленных параметров конфигурации устанавливаются в эксплуатационной документации или регламентируются внутренним документом Оператора, при этом проверки должны проводиться не реже чем раз в год.

10.8. Пользователи и обслуживающий персонал ИСПДн не должны осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование ПДн. С этой целью организационно-техническими мерами запрещено несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование ПДн, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки.

10.9. Процессы обработки ПДн, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются разработчиком ИСПДн в проектной и эксплуатационной документации.

10.10. Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечиваются по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов. Количество последовательных неудачных попыток ввода пароля должно быть ограничено - от 3 до 5 попыток. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности.

Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком ИСПДн в эксплуатационной документации в инструкциях (руководствах) администраторов информационной безопасности.

10.11. Передача ПДн должна осуществляться только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию с ответственным сотрудником по обеспечению информационной безопасности.

10.12. Выполнение функций обеспечения безопасности ПДн в ИСПДн должно обеспечиваться средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО).

10.13. На стадии ввода в действие разработчиком ИСПДн должны быть выполнены настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий. Разработчиком ИСПДн должен быть определен порядок постоянного контроля фактического состояния указанных настроек на предмет их соответствия установленным правилам. Указанный порядок должен быть согласован с ответственным сотрудником по информационной безопасности.

10.14. Регистрация входа в ИСПДн (выхода из ИСПДн) субъекта доступа является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

- дата и время входа в систему (выхода из системы) субъекта доступа;
- идентификатор субъекта, предъявленный при запросе доступа;
- результат попытки входа: успешная или неуспешная (несанкционированная);
- идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

10.15. Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив. Операция по архивированию журнала регистрации событий должна, в свою очередь, регистрироваться с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

10.16. Оператором определен и документально зафиксирован порядок постановки на учет и снятия с учета машинных носителей, предназначенных для размещения ПДн. Снятие с учета машинных носителей, на которых были размещены ПДн, производится по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения. Процедура стирания информации регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн в зависимости от применяемого средства гарантированного стирания.

10.17. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован. Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован. Соответствующие регламенты в виде инструкций и руководств готовятся разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

10.18. Сохранность и целостность программных средств ИСПДн и ПДн являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн. Средства восстановления функций обеспечения безопасности ПДн в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств. Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий, регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

10.19. Восстановление функций обеспечения безопасности ПДн в ИСПДн в случае нештатной ситуации должно осуществляться системным администратором ИСПДн с обязательным привлечением ответственного сотрудником по информационной безопасности. Процедура восстановления должна быть регламентирована разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

10.20. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые обеспечивают выполнение следующих функций:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- возможность проверки (контроля) целостности программной и информационной частей средства межсетевого экранирования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);
- возможность проведения регламентного тестирования реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления (в том числе с

применением внешних программных средств, не встроенных в средство межсетевого экранирования).

11. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПДн

11.1. Лица, виновные в нарушении положений законодательства РФ в области ПДн при их обработке, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

11.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки ПДн, а также несоблюдения требований к защите ПДн, установленных Федеральным законом от 27.07.2006 N 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

Данное Положение вступает в силу со дня подписания и отменяет действие предыдущей редакции.

Приложение 1

УТВЕРЖДАЮ:

Генеральный директор

ООО НКО «Тайдон»

_____ М.В. Наумова

«_____» _____ 20__г.

Перечень лиц, доступ которых к ИСПДн необходим для выполнения ими служебных обязанностей.

№ п/п	Должность	ФИО	Роспись

Приложение 2

Журнал учета обращений граждан (субъектов ПДн) по вопросам обработки ПДн ООО НКО «Тайдон»

Журнал начат «___» _____ 20___ Журнал завершен «____» _____ 20___
На _____ листах

№ п/п	Сведения о запрашивающем лице	Содержание обращения	Цель запроса	Отметка о предоставлении (отказе) информации	Дата передачи (отказа) предоставления информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Ответственный сотрудник
по информационной безопасности

Приложение 3

Утверждаю
Генеральный директор
ООО НКО "Тайдон"
_____М.В. Наумова
«_____» _____ 20___ г.

Список информационных систем ООО НКО "Тайдон", в которых обрабатываются ПДн

№ п/п	Наименование системы	Цель создания ИСПДн	Эксплуатирующее ИСПДн подразделение	Исходные данные	Примечания

Приложение 4

Утверждаю:
Генеральный директор
ООО НКО "Тайдон"

_____ М.В. Наумова

«____» _____ 20____ г.

Акт классификации ИСПДн ООО НКО «Тайдон»

№ п/п	Наименование ИСПДн	Цель создания ИСПДн (цель обработки ПДн)	Эксплуатирующее ИСПДн подразделение	Исходные данные ИСПДн	Класс ИСПДн	Общий класс ИСПДн
1	2	3	4	5	6	

Приложение 5

Генеральному директору
ООО НКО "Тайдон"
М.В. Наумовой

от _____

_____

Согласие на обработку персональных данных

В соответствии с требованиями Федерального закона «О персональных данных» №152-ФЗ от 27.07.2006г. я, гражданин/гражданка РФ,

_____

дата рождения: _____, паспорт серии _____ номер _____

выдан _____

_____

адрес:_____

свободно, своей волей и в своем интересе даю согласие ООО НКО "Тайдон" ИНН 4207013490 КПП 420501001 ОГРН 1024200685948 (юридический адрес: 650070, г. Кемерово, пр. Молодежный, д. 5) на обработку, хранение и использование моих персональных данных, а именно:

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения о занимаемых ранее должностях и стаже работы;
- сведения о воинской обязанности, воинском учете;
- фотография;
- адрес регистрации;
- адрес проживания;
- сведения о семейном положении и составе семьи;
- сведения об имущественном положении, доходах, задолженности;
- сведения об образовании, профессии, специальности и квалификации, реквизиты документов об образовании;
- сведения о состоянии здоровья, связанные с возможностью выполнения трудовой функции;
- контактные данные (номер телефона, адрес электронной почты), то есть на совершение действий, предусмотренных п.3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с целью обеспечения соблюдения законов и иных нормативных правовых актов, исполнения трудового договора, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работников и работодателя.

Если мои персональные данные можно получить только у третьей стороны, то я должен быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных, также должно быть получено на это согласие.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе, моя обязанность проинформировать ООО НКО «Тайдон» в случае изменения моих персональных данных.

Под обработкой персональных данных я понимаю сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение и любые другие действия (операции) с персональными данными в рамках законодательства РФ.

Настоящее заявление может быть отозвано мной в письменной форме на имя генерального директора, по почте в адрес ООО НКО «Тайдон» заказным письмом с уведомлением о вручении или лично - в таком случае ООО НКО "Тайдон" может начать процедуру расторжения трудового договора.

Настоящее согласие действует со дня его подписания и до дня отзыва в письменной форме.

"____"_____ _____ г.

Субъект персональных данных:

_____/_____

(подпись) (Ф.И.О.)

Приложение 6

Генеральному директору
ООО НКО «Тайдон»
Наумовой М.В.

от _____
(фамилия, имя, отчество)

_____
(почтовый адрес субъекта персональных данных)

_____
(номер телефона)

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения

Я,

_____,
(фамилия имя отчество полностью)

в соответствии со ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", в целях:

_____

_____

даю согласие ООО НКО "Тайдон" ИНН 4207013490 КПП 420501001 ОГРН 1024200685948 (юридический адрес: 650070, г. Кемерово, пр-кт Молодежный, д. 5, сведения об информационных ресурсах Оператора: https://www.taidon.ru/), на обработку в форме распространения моих персональных данных, а именно размещение информации обо мне на официальном сайте _____ - https://_____
_

Категории и перечень моих персональных данных, на обработку в форме распространения которых я даю согласие:

☐ Перечень моих персональных данных, на распространение которых я даю согласие:

- фамилия, имя, отчество;

_____

_____

_____

_____

_____

_____

☐ Биометрические персональные данные:

- фотографическое изображение.

Условия и запреты на обработку вышеуказанных персональных данных (ч. 9 ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных") (нужное отметить):

- ☐ не устанавливаю
- ☐ устанавливаю запрет на передачу (кроме предоставления доступа) этих данных Оператором неограниченному кругу лиц
- ☐ устанавливаю запрет на обработку (кроме получения доступа) этих данных неограниченным кругом лиц
- ☐ устанавливаю условия обработки (кроме получения доступа) этих данных неограниченным кругом лиц:

_____

_____

Условия, при которых полученные персональные данные могут передаваться Оператором только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных:

_____

_____

Настоящее согласие дано мной добровольно и действует со дня его подписания до

_____

(указать дату)

Субъект персональных данных:

_____/_____

(подпись) (Ф.И.О.)

"____"_____ ____ г.