

**Небанковская кредитная организация «Расчетно-кассовый центр**

**«Дальний Восток» (Акционерное общество)**

|  |  |
| --- | --- |
|  | **УТВЕРЖДЕНО**  **Решением Правления**  **НКО «РКЦ ДВ» (АО)**  **Протокол заседания Правления**  **№ 66 от «29» декабря 2023 г.**  **Председатель Правления**    **\_\_\_\_\_\_\_\_\_\_\_ /А.В. Хаников/** |

**ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**В НКО «РКЦ ДВ» (АО)**

г. Владивосток

**СОДЕРЖАНИЕ**

|  |  |  |
| --- | --- | --- |
| 1 | Термины, определения, сокращения, используемые в документе………………… | 3 |
| 2 | Общие положения…………………………………………………………………….. | 5 |
| 3 | Цели и принципы обработки персональных данных………………………………. | 6 |
| 4 | Категории субъектов ПДн, объем обрабатываемых ПДн………………………….. | 7 |
| 5 | Порядок и условия обработки ПДн………………………………………………….. | 9 |
| 6 | Актуализация, уточнение, блокирование и уничтожение ПДн……………………. | 18 |
| 7 | Права и обязанности НКО и субъектов персональных данных…………………… | 20 |
| 8 | Порядок представления субъектом ПДн\его представителем заявлений о неточности ПДн, неправомерности их обработки, доступе к своим персональным данным и отзыва согласия на их обработку……………………….. | 21 |
| 9 | Меры, направленные на обеспечение выполнения обязанностей по обработке и защите ПДн……………………………………………………………………………. | 22 |
| 10 | Основной функционал лица, ответственного за организацию и функционирование системы обработки ПДн в НКО………………………………. | 22 |
| 11 | Осуществление внутреннего контроля в области обработки персональных данных…………………………………………………………………………………. | 23 |
| 12 | Порядок оценки уровня\степени вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ «О персональных данных»……………... | 24 |
| 13 | Заключительные положения…………………………………………………………. | 26 |
| 14 | Приложения…………………………………………………………………………… | 27 |

1. **ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ДОКУМЕНТЕ**

|  |  |
| --- | --- |
| **НКО** | НКО «РКЦ ДВ» (АО), являющаяся в рамках Федерального закона № 152-ФЗ оператором по обработке ПДн, организующим и\или осуществляющим самостоятельно или совместно с другими лицами обработку персональных данных, а также определяющим цели обработки ПДн, состав ПДн, подлежащих обработке, действия\операции, совершаемые с ПДн |
| **Работник НКО** | физическое лицо, заключившее с НКО трудовой договор\договор ГТХ |
| **Персональные данные или ПДн** | любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн) |
| **Персональные данные, разрешенные субъектом персональных данных для распространения** | персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения [в порядке](#sub_1010), предусмотренном Федеральным законом № 152-ФЗ |
| **Оператор** | государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными |
| **Субъект ПДн** | физическое лицо, которое прямо или косвенно определено с помощью персональных данных |
| **Обработка персональных данных** | любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных |
| **Автоматизированная обработка персональных данных** | обработка персональных данных с помощью средств вычислительной техники\*  \* под средствами вычислительной техники понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. То есть в понятие "средства вычислительной техники" инкорпорированы:   1. компьютерные системы, 2. автоматизированные системы обработки информации, 3. системы программного обеспечения и т. п. элементы.   В п. "с" ст. 2 Конвенции Совета Европы N 108 "О защите частных лиц в отношении автоматизированной обработки данных личного характера" указано, что "***автоматизированная обработка***" включает в себя следующие операции, осуществляемые полностью или частично с помощью автоматизированных средств:   1. хранение данных, 2. осуществление логических и/или арифметических операций с этими данными, 3. их изменение, уничтожение, поиск или распространение.   Если подобные действия в отношении конфиденциальной информации, содержащей персональные данные, совершаются в автоматическом режиме (например, программа после подачи специалистом определенной команды без участия человека обращается к своей базе данных, хранящих соответствующие персональные данные субъектов, систематизирует их и выдает по установленному алгоритму результат), то ***такая обработка персональных данных будет считаться автоматизированной,*** ***даже если изначально персональные данные субъектов вводятся в информационную систему и впоследствии выгружаются из нее вручную человеком*** |
| **Неавтоматизированная обработка персональных данных** | *в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным*[*постановлением*](https://internet.garant.ru/#/document/193875/entry/0)*Правительства РФ от 15.09.2008 N 687:*   1. обработка персональных данных, содержащихся в информационной системе ПДн либо извлеченных из нее, считается неавтоматизированной, если такие операции с персональными данными, как использование, уточнение, распространение, уничтожение (в отношении каждого из субъектов ПДн), осуществляются при непосредственном участии человека; 2. обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что эти данные содержатся в информационной системе персональных данных либо извлечены из нее. |
| **Распространение персональных данных** | действия, направленные на раскрытие персональных данных неопределенному кругу лиц |
| **Передача\предоставление персональных данных** | действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц |
| **Блокирование персональных данных** | временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) |
| **Уничтожение персональных данных** | действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных |
| **Обезличивание персональных данных** | действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных |
| **Информационная система персональных данных\ИСПДн** | совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств |
| **Трансграничная передача персональных данных** | передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу |
| **Биометрические персональные данные** | сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн |
| **Информация** | сведения (сообщения, данные) независимо от формы их представления |
| **Конфиденциальность ПДн** | обязательное для соблюдения сотрудниками НКО или иными лицами, получившими доступ к ПДн, требование не раскрывать третьим лицам и не распространять без согласия Субъекта ПДн его персональные данные |
| **Ответственное лицо** | должностное лицо НКО, назначенное Единоличным исполнительным органом (директором) НКО ответственным за организацию и функционирование системы обработки персональных данных |
| **Уполномоченный орган по защите прав субъектов персональных данных** | Роскомнадзор |
| **Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности** | ФСБ |
| **Федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации** | ФСТЭК |
| **Угрозы безопасности ПДн** | совокупность условий и факторов, создающих опасность несанкционированного, в т.ч. случайного, доступа к ПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия при их обработке в информационной системе ПДн |
| **Уровень защищенности ПДн** | комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в ИСПДн |

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

2.1. Настоящее Положение разработано в целях реализации требований действующего российского законодательства в области обработки и обеспечения безопасности персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в НКО.

* 1. Настоящее Положение устанавливает:

1. цели обработки персональных данных;
2. классификацию персональных данных и Субъектов персональных данных;
3. общие принципы обработки персональных данных;
4. основных участников системы управления процессом обработки персональных данных;
5. основные подходы к системе управления процессом обработки персональных данных.

2.3. Положения настоящего документа являются основой для организации работы по обработке персональных данных в НКО, в том числе, для разработки внутренних документов, (регламентов методик, технологических схем и пр.), регламентирующих процесс обработки персональных данных, и являются обязательными для исполнения всеми работниками НКО, имеющими доступ к персональным данным.

2.4. Работники НКО, а также лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия Субъекта ПДн, если иное не предусмотрено федеральным законом (права, обязанности и ответственность Пользователей ИСПДн представлены в Приложении № 5 к настоящему Положению).

2.5. Настоящее Положение размещается на сайте НКО в информационно-телекоммуникационной сети «Интернет».

**3. ЦЕЛИ И ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

***3.1. Основные принципы обработки ПДн в НКО:***

(1) обработка ПДн осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей;

(2) обработка ПДн, не совместимая с целями сбора персональных данных, не допускается;

(3) не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, не совместимых между собой;

(4) обработке подлежат только ПДн, которые отвечают целям их обработки;

(5) содержание и объем обрабатываемых ПДн соответствует заявленным целям обработки, не допускается их избыточность;

(6) при обработке ПДн обеспечиваются точность ПДн, их достаточность и актуальность по отношению к целям их обработки;

(7) если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, хранение ПДн осуществляется в форме, позволяющей определить Субъекта ПДн, не дольше, чем того требуют цели обработки ПДн;

(8) обрабатываемые ПДн уничтожаются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

***3.2. НКО осуществляет обработку персональных данных в целях:***

(1) осуществления банковских операций в соответствии с Уставом НКО и выданной ей лицензией на совершение банковских операций и других сделок;

(2) заключения, исполнения и прекращения гражданско-правовых договоров с Субъектами персональных данных;

(3) ведения кадровой работы и организации кадрового учета работников НКО;

(4) привлечения и отбора кандидатов на вакантные должности;

(5) формирования отчетности, в том числе для предоставления Банку России;

(6) осуществления НКО административно-хозяйственной деятельности;

(7) регулирования трудовых и иных, непосредственно связанных с ними отношений;

(8) выявления случаев мошенничества, хищения денежных средств со счета, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий;

(9) в иных законных целях.

**4. КАТЕГОРИИ СУБЪЕКТОВ ПДн, ОБЪЕМ ОБРАБАТЫВАЕМЫХ ПДн**

***4.1. НКО обрабатывает персональные данные следующих категорий Субъектов ПДн:***

(1) физических лиц, являющихся работниками\кандидатами на вакантные должности в НКО;

(2) физических лиц – представителей юридических лиц:

(а) входящих в органы управления НКО;

(б) входящих в органы управления юридического лица, являющегося аффилированным по отношению к НКО\контролирующим лицом и\или являющихся учредителями\акционерами НКО;

(в) являющихся работниками юридического лица, аффилированного по отношению к НКО;

(3) физических лиц, представляющих интересы юридического лица, являющегося клиентом\контрагентом НКО на основании заключенного с НКО договора (в т.ч. договора, заключенного путем присоединения к условиям публичного договора), договора, обеспечивающего обязательства другого физического\юридического лица перед НКО;

(4) физических лиц, в т.ч. являющихся представителями юридического лица, заключивших или намеревающихся заключить с НКО договоры гражданско-правового характера, в связи с осуществлением НКО административно-хозяйственной деятельности, т.е. деятельности, направленной на текущее обеспечение деятельности НКО товарно-материальными ценностями, организацию документооборота, организацию рабочего процесса и т.д.;

(5) физических лиц, пользующихся или намеревающихся пользоваться услугами НКО, услугами третьих лиц при посредничестве НКО, или не имеющих с НКО договорных отношений, при условии, что их ПДн включены в автоматизированные системы (АБС) НКО и обрабатываются в соответствии с требованиями законодательства о персональных данных;

(6) физических лиц, ПДн которых разрешены ими для передачи\распространения, а их обработка не нарушает их прав и соответствует требованиям, установленным законодательством о персональных данных;

(7) иных физических лиц, выразивших согласие на обработку НКО их ПДн, или физических лиц, обработка ПДн которых необходима НКО для осуществления и выполнения ею возложенных законодательством РФ функций, полномочий и обязанностей.

***4.2. НКО в зависимости от целей обработки и категории Субъектов ПДн осуществляет обработку следующих ПДн:***

(1) фамилия, имя, отчество (при наличии);

(2) дата рождения;

(3) адрес регистрации\места проживания;

(4) образование;

(5) сведения о работе;

(6) номер банковского счета;

(7) № телефона, адрес электронной почты;

(8) СНИЛС;

(9) ИНН;

(10) паспортные данные\данные заграничного паспорта;

(11) другие ПДн.

|  |  |
| --- | --- |
| ***Категории субъектов ПДн*** | ***Перечень (объем) обрабатываемых ПДн*** |
| *1. физические лица – представители юридических лиц:*  *(а) входящих в органы управления НКО;*  *(б) входящих в органы управления юридического лица, являющегося аффилированным по отношению к НКО\контролирующим лицом и\или являющихся учредителями\акционерами НКО;*  *(в) являющихся представителями юридического лица, аффилированного по отношению к НКО* | *1. Фамилия, имя, отчество (при наличии) акционера*  *(участника) - физического лица*  *2. Место нахождения (место жительства) акционера*  *(участника)\ почтовый адрес (для направления*  *корреспонденции)*  *3. Наименование и реквизиты документа,*  *удостоверяющего личность акционера (участника)*  *4. Количество голосов, принадлежащих акционеру*  *(участнику)* |
| *2. физические лица, представляющие интересы юридического лица, являющегося клиентом\контрагентом НКО на основании заключенного с НКО договора (в т.ч. договора, заключенного путем присоединения к условиям публичного договора), договора, обеспечивающего обязательства другого физического\юридического лица перед НКО;* | *Идентификационные сведения, установленные Федеральным законом № 115-ФЗ «О противодействии легализации…», Положением Банка России № 499-П, внутренними ПВК по ПОД\ФТ\ФРОМУ* |
| *3. физические лица, в т.ч. являющиеся представителями юридического лица, заключившие или намеревающиеся заключить с НКО договоры, в т.ч. гражданско-правового характера в связи с осуществлением НКО административно-хозяйственной деятельности, т.е. деятельности, направленной на текущее обеспечение деятельности НКО товарно-материальными ценностями, организацию документооборота, организацию рабочего процесса и т.д.* | *Идентификационные сведения, установленные Федеральным законом*  *№ 115-ФЗ «О противодействии легализации…», Положением Банка России № 499-П, внутренними ПВК по ПОД\ФТ\ФРОМУ* |
| *4. физические лица, пользующиеся или намеревающиеся пользоваться услугами НКО, услугами третьих лиц при посредничестве НКО, или не имеющие с НКО договорных отношений, при условии, что их ПДн включены в автоматизированные системы (АБС) НКО и обрабатываются в соответствии с требованиями законодательства о персональных данных* | *Идентификационные сведения, установленные Федеральным законом № 115-ФЗ «О противодействии легализации…», Положением Банка России № 499-П, внутренними ПВК по ПОД\ФТ\ФРОМУ* |
| *5. физические лица, являющиеся кандидатами на вакантные должности\сотрудниками НКО* | *1. Фамилия, имя, отчество (при наличии)*  *2. Дата рождения*  *3. ИНН*  *4. СНИЛС*  *5. № телефона\адрес электронной почты*  *6. Образование*  *7. Наличие судимости*  *8. Отношение к воинской обязанности*  *9. Сведения о работе*  *10. Адрес регистрации\места*  *проживания\пребывания*  *10. Сведения о составе семьи\близких родственниках*  *(супруг\супруга, родители, дети, братья\сестры)* |

**4.3.** ***В целях информационного обеспечения и соблюдения требований законодательства РФ НКО с письменного согласия Субъектов ПДн*** вправе создавать общедоступные источники ПДн (в т.ч. справочники, адресные книги), содержащие ФИО, год рождения, адрес, сведения о должности и иные ПДн, сообщаемые Субъектом.

**5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПДн**

***5.1. НКО обрабатывает ПДн только при наличии хотя бы одного из следующих условий:***

**(1)** ***обработка ПДн осуществляется с согласия Субъекта ПДн*** на обработку его персональных данных (кроме случаев, установленных законодательством РФ, разрешающих обработку ПДн без согласия Субъекта) с соблюдением требований конфиденциальности, а также принятием мер, направленных на обеспечение выполнения обязанностей по обработке и защите ПДн, установленных законодательством Российской Федерации.

При этом:

(а) ***трансграничная передача*** персональных данных (в случае возникновения такой необходимости) ***осуществляется только при наличии согласия в письменной форме*** Субъекта ПДн, оформленного в соответствии с п. 4 ст. 9 Закона № 152-ФЗ;

(б) обработка ПДн, разрешенных Субъектом ПДн для ***передачи\распространения***, осуществляется на основании ***согласия***, которое ***оформляется отдельно от иных согласий*** Субъекта персональных данных.

В данном согласии Субъект имеет право определить перечень ПДн по каждой категории персональных данных, указанной в согласии на их обработку, разрешенных Субъектом ПДн для передачи\распространения, установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц;

(в) обработка персональных данных Субъектов, не достигших совершеннолетия, осуществляется при наличии согласия законного представителя такого субъекта;

***(2)******обработка*** *персональных данных* ***необходима для достижения целей****, предусмотренных* ***международным договором*** *Российской Федерации или* ***законом****, для осуществления и выполнения возложенных законодательством РФ на НКО функций, полномочий и обязанностей;*

***(3)*** *обработка персональных данных необходима* ***для исполнения договора****, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн, а также для заключения договора по инициативе Субъекта или договора, по которому Субъект будет являться выгодоприобретателем или поручителем;*

**(4)** обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта персональных данных, если получение его согласия невозможно;

***(5)*** *обработка ПДн необходима для осуществления прав и законных интересов НКО или третьих лиц в случаях, предусмотренных законом при условии, что при этом не нарушаются права и свободы Субъекта ПДн;*

**(6)** требования к содержанию согласия на обработку персональных данных, разрешенных Субъектом ПДн для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных (Роскомнадзором);

**(7)** осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

***5.2. Порядок уведомления уполномоченного органа по защите прав Субъектов ПДн (Роскомнадзор):***

5.2.1. НКО (Лицо, ответственное за организацию обработки ПДн, либо иное лицо, назначенное Директором НКО) до начала обработки ПДн, уведомляет уполномоченный орган по защите прав Субъектов ПДн о своем намерении осуществлять обработку персональных данных, ***за исключением следующих случаев:***

(1) осуществление обработки персональных данных в соответствии с трудовым законодательством;

(2) осуществление обработки персональных данных в связи с заключением договора, стороной которого является Субъект ПДн (если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия Субъекта персональных данных и используются НКО исключительно для исполнения указанного договора и заключения договоров с Субъектами ПДн);

(3) осуществление обработки персональных данных, разрешенных Субъектом ПДн для распространения, при условии соблюдения НКО запретов и условий, предусмотренных статьей 10.1 Закона № 152-ФЗ;

(4) осуществление обработки ПДн, включающих в себя только фамилии, имена и отчества субъектов персональных данных;

(5) осуществление обработки персональных данных, необходимых в целях однократного пропуска Субъекта ПДн на территорию НКО или в иных аналогичных целях;

(6) осуществление обработки персональных данных, включенных в информационные системы персональных данных, имеющих в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

(7) осуществление обработки персональных данных без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав Субъектов персональных данных;

(8) в иных предусмотренных законом случаях.

5.2.2. Содержание и порядок направления уведомления уполномоченному органу по защите прав Субъектов ПДн должны соответствовать требованиям действующего законодательства.

5.2.3. В случае изменения ранее представленных сведений или в случае прекращения обработки персональных данных НКО ***в течение 10 (десяти) рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных*** направляет в уполномоченный орган по защите прав Субъектов ПДн (Роскомнадзор) Информационное письмо, форма которого установлена Приложением 2 к Методическим рекомендациям по уведомлению уполномоченного органа о начале деятельности по обработке персональных данных и внесении изменений в ранее представленные сведения (утв. Приказом Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»).

***5.3. Перечень действий и способов обработки персональных данных:***

5.3.1. НКО вправе использовать при обработке персональных данных Субъекта ПДн автоматизированный, механический, ручной и любой иной способ по своему усмотрению.

5.3.2. НКО осуществляет любое действие (операцию) или совокупность действий (операций) с персональными данными Субъекта, включая:

(1) сбор,

(2) запись,

(3) систематизацию,

(4) накопление,

(4) хранение,

(5) уточнение (обновление, изменение),

(6) извлечение,

(7) использование,

(8) передачу (предоставление, доступ),

(9) распространение,

(10) блокирование,

(11) удаление,

(12) уничтожение персональных данных,

если иное не предусмотрено законом или не содержится в согласии Субъекта на обработку персональных данных.

5.3.3. Перечень должностей и\или структурных подразделений НКО, осуществляющих обработку персональных данных, утверждается Директором НКО\лицом его замещающим (Приложение 7 к настоящему документу).

5.3.4. Обработка персональных данных Субъектов ПДн без использования средств автоматизации (далее – неавтоматизированная обработка), осуществляется на бумажных и машинных носителях информации (далее по тексту – материальный носитель информации).

При неавтоматизированной обработке различных категорий персональных данных для каждой категории используется отдельный материальный носитель.

***5.4. Сбор\получение персональных данных***

5.4.1. Все персональные данные Субъекта ПДн НКО получает непосредственно у Субъекта либо его законного представителя, если иное не предусмотрено законодательством Российской Федерации.

5.4.2. Решение Субъекта о представлении своих персональных данных должно быть добровольным, какое-либо давление на него недопустимо.

5.4.3. Принимая решение о предоставлении своих данных, Субъект ПДн дает согласие на их обработку, в случае если такое согласие необходимо в соответствии с действующим законодательством Российской Федерации. ***Согласие должно быть конкретным, информированным и осознанным.***

5.4.4. Типовые формы Согласия представлены в Приложениях № 2, 2-а, 2-б, 2-в к настоящему Положению.

При возникновении ранее отсутствовавших (новых) целей обработки ПДн разрабатываются новые формы Согласия.

5.4.5. Если персональные данные Субъекта возможно получить только у третьей стороны, то эта третья сторона должна быть уведомлена об этом заранее и от нее должно быть получено письменное согласие.

Работник НКО должен сообщить Субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта дать письменное согласие на их получение.

5.4.6. Персональные данные могут быть получены НКО от лица, не являющегося Субъектом ПДн, при условии представления НКО подтверждения наличия оснований, указанных в п.2 -11 ч.1 ст.6 Закона № 152-ФЗ (например, выполнение требований ФЗ «О противодействии легализации…».

5.4.7. В случае недееспособности Субъекта согласие на обработку его персональных данных дает законный представитель Субъекта.

5.4.8. В случае смерти Субъекта согласие на обработку его персональных данных дают наследники Субъекта, если такое согласие не было дано Субъектом при его жизни.

***5.5. Хранение персональных данных.***

5.5.1. Хранение персональных данных — это процесс, регулируемый законодательством, решением владельца и целями использованиясведений.

5.5.2. Хранение персональных данных осуществляется в форме, позволяющей определить Субъекта ПДн не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Субъект персональных данных.

5.5.3. При осуществлении хранения персональных данных НКО может использовать базы данных, находящиеся на территории Российской Федерации.

5.5.4. Хранимые персональные данные подлежат защите от несанкционированного доступа и копирования.

Безопасность персональных данных при их хранении обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

5.5.5. Хранение персональных данных НКО обеспечивается:

(1) проведением мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и\или передачи их лицам, не имеющим права доступа к такой информации;

(2) своевременным обнаружением фактов несанкционированного доступа к персональным данным;

(3) недопущением воздействия на технические средства автоматизированной обработки персональных данных или на бумажные носители, в результате которого может быть нарушено их функционирование;

(4) возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.5.6. Места хранения для каждой категории материальных носителей утверждаются Директором НКО или лицом, его замещающим (Приложение № 1 к настоящему Положению).

5.5.7. Сроки хранения персональных данных в информационных системах ПДн аналогичны срокам хранения персональных данных на материальных (бумажных) носителях.

5.5.8. По истечении срока хранения персональные данные уничтожаются в информационных системах и уничтожаются на материальном (в т.ч. бумажном) носителе.

5.5.9. Хранение персональных данных на бумажных и\или электронных носителях осуществляется НКО в сейфах, запирающихся шкафах, специально оборудованных хранилищах, специально оборудованных помещениях, в помещениях, оборудованных сигнализацией, в помещениях, оснащенных системами видеонаблюдения.

5.5.10. Особенности хранения персональных данных при их обработке без использования средств автоматизации:

(1) обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

(2) при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

***5.6. Передача персональных данных третьим лицам.***

5.6.1. НКО вправе поручить обработку персональных данных другому лицу с согласия Субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

Лицо, осуществляющее обработку персональных данных по поручению НКО, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом № 152-ФЗ «О персональных данных».

5.6.2. Персональные данные не раскрываются третьим лицам и не распространяются иным образом без согласия Субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

При раскрытии (предоставлении) персональных данных третьим лицам соблюдаются требования к защите обрабатываемых персональных данных.

5.6.3 Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных, дознания и следствия и иных уполномоченных органов по основаниям, предусмотренным действующим законодательством Российской Федерации) получают доступ к персональным данным, обрабатываемым в НКО, в объеме и порядке, установленном законодательством Российской Федерации.

Представление сведений, относящихся в соответствии с действующим законодательством Российской Федерации к банковской тайне, третьим лицам осуществляется в соответствии с законодательством РФ и внутренними документами НКО.

***5.7. Трансграничная передача персональных данных:***

5.7.1. В соответствии с требованиями ст. 12 Закона № 152-ФЗ НКО вправе (может) осуществлять трансграничную передачу ПДн.

5.7.2. Уполномоченный орган по защите прав Субъектов ПДн (Роскомнадзор) утверждает [перечень](https://internet.garant.ru/#/document/405309273/entry/1000) иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

В указанный перечень включаются государства, являющиеся сторонами [Конвенции](https://internet.garant.ru/#/document/2559798/entry/0) Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иностранные государства, не являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер по обеспечению конфиденциальности и безопасности персональных данных при их обработке.

5.7.3. До начала осуществления деятельности по трансграничной передаче персональных данных НКО обязана уведомить Роскомнадзор о своем намерении осуществлять трансграничную передачу ПДн (указанное уведомление направляется отдельно от уведомления о намерении осуществлять обработку персональных данных, предусмотренного [статьей 22](https://internet.garant.ru/#/document/12148567/entry/22)  Федерального закона № 152-ФЗ).

5.7.4. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом НКО.

Уведомление о намерении осуществлять трансграничную передачу персональных данных должно содержать следующие сведения:

1. наименование НКО,
2. адрес НКО,
3. дата и номер уведомления о намерении осуществлять обработку персональных данных, ранее направленного НКО в соответствии со [статьей 22](https://internet.garant.ru/#/document/12148567/entry/22)  Федерального закона № 152-ФЗ;
4. наименование (фамилия, имя, отчество) лица, ответственного за организацию обработки ПДн, номера контактных телефонов, почтовые адреса и адреса электронной почты;
5. правовое основание и цель трансграничной передачи персональных данных и дальнейшей обработки переданных ПДн;
6. категории и перечень передаваемых персональных данных;
7. категории субъектов ПДн, персональные данные которых передаются;
8. перечень иностранных государств, на территории которых планируется трансграничная передача персональных данных;
9. дата проведения НКО оценки соблюдения органами власти иностранных государств, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача ПДн, конфиденциальности персональных данных и обеспечения безопасности ПДн при их обработке.

5.7.5. До подачи уведомления необходимо получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача ПДн, следующие сведения:

(1) о принимаемых органами власти иностранного государства, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, мерах по защите передаваемых персональных данных и об условиях прекращения их обработки;

(2) о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находятся органы власти иностранного государства, иностранные физические лица, иностранные юридические лица, которым планируется трансграничная передача персональных данных (в случае, если предполагается осуществление трансграничной передачи персональных данных органам власти иностранного государства, иностранным физическим лицам, иностранным юридическим лицам, находящимся под юрисдикцией иностранного государства, не являющегося стороной [Конвенции](https://internet.garant.ru/#/document/2559798/entry/0) Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных);

(3) об органах власти иностранного государства, иностранных физических лицах, иностранных юридических лицах, которым планируется трансграничная передача персональных данных (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты).

5.7.6. В целях оценки достоверности сведений, содержащихся в уведомлении НКО о своем намерении осуществлять трансграничную передачу персональных данных, сведения, предусмотренные подпунктами 1-3 пункта 5.7.5 настоящего Положения, предоставляются НКО по запросу уполномоченного органа по защите прав Субъектов ПДн (Роскомнадзора) в течение десяти рабочих дней с даты получения такого запроса.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

***5.8. Требования, которые необходимо соблюдать при передаче персональных данных:***

(1) не сообщать ПДн в коммерческих целях;

(2) осуществлять передачу персональных данных в пределах НКО в соответствии с настоящим Положением, должностными инструкциями сотрудников, внутренними распорядительными актами (приказами\распоряжениями);

(3) передавать персональные данные Субъекта ПДн представителям в порядке, установленном Трудовым кодексом Российской Федерации, иными федеральными законами, и ограничивать эту информацию только теми персональными данными Субъекта, которые необходимы для выполнения указанными представителями их функций.

**5.9.** ***Сроки обработки персональных данных*** определяются в соответствии со сроком, указанным в согласии Субъекта ПДн, а также в соответствии со сроками, установленными государственными органами РФ, сроками исковой давности, а также иными требованиями законодательства Российской Федерации и нормативными документами Банка России.

Сроки обработки персональных данных доводятся до Субъекта ПДн в момент подписания им согласия на обработку персональных данных.

**5.10.** ***Типовые формы документов НКО*** *(как правило, договоров),* содержащих сведения о Субъектах персональных данных и\или согласия таких Субъектов, утверждаются Директором или иным уполномоченным лицом и содержатся во внутренних документах НКО, регулирующих отношения НКО с той или иной категорией Субъектов ПДн.

Типовые формы документов НКО используются в соответствии с требованиями, установленными Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

***Справочный комментарий:***

***Под типовыми формами документов НКО понимается шаблон, бланк документа и пр., используемые с целью сбора персональных данных.***

**6. АКТУАЛИЗАЦИЯ, УТОЧНЕНИЕ, БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ ПДн**

6.1. НКО осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к Субъекту ПДн, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению НКО) с момента такого обращения или получения указанного запроса на период проверки:

(1) в случае выявления неправомерной обработки персональных данных при обращении Субъекта ПДн или его представителя;

(2) в случае выявления неточных персональных данных (если блокирование персональных данных не нарушает права и законные интересы Субъекта ПДн или третьих лиц);

(3) по запросу Субъекта ПДН или его представителя либо уполномоченного органа по защите прав Субъектов персональных данных.

**6.2**. ***В случае подтверждения факта неточности персональных данных*** (на основании сведений, представленных Субъектом ПДн или его представителем либо Роскомнадзором, или на основании иных необходимых документов) НКО уточняет персональные данные либо обеспечивает их уточнение (если обработка ПДн осуществляется другим лицом, действующим по ее поручению) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации осуществляется путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя − путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

***6.4. НКО уничтожает персональные данные в следующих случаях:***

(1) при представлении Субъектом ПДн\его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки – не позднее семи рабочих дней со дня представления таких сведений (п. 1 ст. 14, ч. 3 ст. 20 Закона № 152-ФЗ);

(2) при выявлении неправомерной обработки персональных данных, если невозможно обеспечить ее правомерность, – не позднее десяти рабочих дней с даты выявления неправомерной обработки ПДн (п. 3 ст. 21 Закона № 152-ФЗ);

(3) при достижении цели обработки персональных данных – в течение тридцати дней с даты достижения цели обработки ПДн (п. 4 ст. 21 Закона № 152-ФЗ);

(4) при отзыве Субъектом ПДн согласия на обработку его персональных данных, если их сохранение более не требуется для целей обработки персональных данных – в течение тридцати дней с даты поступления указанного отзыва (п. 5 ст. 21 Закона № 152-ФЗ);

При достижении цели обработки персональных данных и при отзыве Субъектом ПДн согласия на обработку его персональных данных применяется другой срок для уничтожения персональных данных Субъекта, если:

1. он предусмотрен договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных;
2. он предусмотрен иным соглашением между НКО и Субъектом ПДн;
3. если НКО не вправе осуществлять обработку персональных данных без согласия Субъекта ПДН по основаниям, предусмотренным Законом № 152-ФЗ или другими федеральными законами (п. 7 ст. 5, п. 4, 5 ст. 21 Закона № 152-ФЗ).

Если у НКО отсутствует возможность уничтожения персональных данных в течение указанных выше сроков (в случаях выявления неправомерной обработки персональных данных или отзыва Субъектом ПДн согласия на их обработку), НКО осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению НКО) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами (Сроки хранения документов, в т.ч. содержащих ПДн, представлены в Приложении № 6 к настоящему документу).

***6.5. Способы уничтожения персональных данных.***

Уничтожение документов (носителей), содержащих персональные данные, может производиться путем:

1. сожжения,
2. дробления (измельчения),
3. химического разложения,
4. превращения в бесформенную массу или порошок.

Для уничтожения бумажных документов допускается применение шредера.

Персональные данные *на электронных носителях* уничтожаются путем стирания или форматирования носителя.

***6.6. Порядок уничтожения персональных данных.***

6.6.1. Уничтожение документов, содержащих ПДн, в т.ч. по окончании срока их хранения, производится специально созданной для этих целей комиссией, назначенной приказом\распоряжением директора НКО.

В состав комиссии (помимо других ее членов) входит лицо, ответственное за обработку ПДн, и лицо, ответственное за безопасность ПДн при их автоматизированной обработке\при проведении работ в ИСПДн.

Уничтожение документов, содержащих ПДн, осуществляется любым выбранным комиссией способом, указанным в п. 6.5.

Результат работы комиссии – факт уничтожения ПДн – подтверждается Актом (Приложение № 7), утвержденным директором НКО.

При уничтожении персональных данных в случае выявления неправомерной их обработки, осуществляемой НКО или лицом, действующим по ее поручению, НКО уведомляет Субъекта ПДн или его представителя об уничтожении персональных данных, а в случае если обращение Субъекта ПДн\его представителя либо запрос уполномоченного органа по защите прав Субъектов персональных данных были направлены уполномоченным органом по защите их прав – также указанный орган.

По истечении срока действия согласия на обработку персональных данных Субъекта, НКО уничтожает те персональные данные, дальнейшая обработка которых не предусмотрена законодательством Российской Федерации.

В случае отзыва Субъектом ПДн согласия на обработку персональных данных НКО вправе продолжить их обработку без согласия Субъекта ПДн при наличии оснований, установленных Законом № 152-ФЗ.

**7. ПРАВА И ОБЯЗАННОСТИ НКО И СУБЪЕКТА ПДн**

**Права и обязанности НКО**:

**7.1**. НКО как оператор персональных данных вправе:

(1) отстаивать свои интересы в суде;

(2) предоставлять (передавать) персональные данные Субъектов третьим лицам, если это предусмотрено действующим законодательством (в налоговые, правоохранительные органы и др.);

(3) отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

(4) использовать персональные данные Субъекта без его согласия, в случаях, предусмотренных законодательством;

(5) требовать от Субъекта ПДн представления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации Субъекта ПДн, а также в иных случаях, предусмотренных законом;

(6) обрабатывать персональные данные, разрешенные Субъектом ПДн для распространения;

(7) осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

**7.2**. НКО как оператор персональных данных обязана:

(1) обрабатывать персональные данные Субъекта в соответствии с заявленной целью в случаях и порядке, установленных действующим законодательством Российской Федерации;

(2) представлять Субъекту ПДн по его просьбе информацию, предусмотренную п. 7 ст. 14 Закона № 152-ФЗ, за исключением случаев, установленных законодательством Российской Федерации;

(3) сообщать в порядке, предусмотренном законом, Субъекту ПДн или его представителю информацию о наличии персональных данных, относящихся к соответствующему Субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении Субъекта ПДн или его представителя;

(4) при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

**Права и обязанности Субъекта ПДн:**

**7.3**. Субъект ПДн имеет право:

(1) требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

(2) получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные законодательством о персональных данных;

(3) получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

(4) требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

(5) обжаловать в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

**8. ПОРЯДОК ПРЕДСТАВЛЕНИЯ СУБЪЕКТОМ ПДн\ЕГО ПРЕДСТАВИТЕЛЕМ ЗАЯВЛЕНИЙ О НЕТОЧНОСТИ ПДн, НЕПРАВОМЕРНОСТИ ИХ ОБРАБОТКИ, ДОСТУПЕ К СВОИМ ПЕРСОНАЛЬНЫМ ДАННЫМ И ОТЗЫВА СОГЛАСИЯ НА ИХ ОБРАБОТКУ**

**8.1.** В целях реализации своих прав, установленных Законом № 152-ФЗ, Субъект ПДн\его представитель вправе представить в НКО заявление о неточности своих персональных данных (персональных данных представляемого лица), неправомерности их обработки, доступе к своим персональным данным (персональным данным представляемого лица) и\или отзыве согласия на обработку своих персональных данных (персональных данных представляемого лица) (далее – Заявление).

Формы вышеуказанных Заявлений представлены в Приложениях №№ 3, 3-а, 3-б к настоящему Положению.

Заявление может быть составлено Субъектом ПДн в свободной форме, но обязательно должно содержать следующие сведения:

(1) номер основного документа, удостоверяющего личность Субъекта ПДн или его представителя,

(2) сведения о дате выдачи указанного документа и выдавшем его органе,

(3) сведения, подтверждающие участие Субъекта ПДн в отношениях с НКО, выступающей в качестве оператора обработки ПДн (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки НКО персональных данных,

(4) подпись Субъекта ПДн или его представителя.

**8.2.** Заявление может быть направлено в форме электронного документа и подписано электронной подписью в соответствии с законодательством Российской Федерации.

Одновременно с подачей Заявления Субъект ПДн предъявляет в НКО документ, удостоверяющий его личность (за исключением случая, когда Заявление представляется в форме электронного документа, подписанного электронной подписью в соответствии с законодательством РФ), а в случае обращения представителя – с предъявлением паспорта представителя и доверенности или иного документа, подтверждающего полномочия представителя Субъекта ПДн.

**8.3**. НКО рассматривает Заявление Субъекта персональных данных\его представителя и готовит на него ответ в соответствии с законодательством Российской Федерации и порядком, установленным внутренними документами НКО.

**9. МЕРЫ, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ ПО ОБРАБОТКЕ И ЗАЩИТЕ ПДн**

**9.1.** НКО самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

**9.2**. Безопасность ПДн обеспечивается в рамках общей системы информационной безопасности НКО посредством соблюдения установленных системой требований (Приложение № 5 к настоящему Положению).

**10. ОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ В ОБЛАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

10.1. Контроль на предмет соответствия обработки ПДн требованиям действующего законодательства осуществляет лицо, ответственное за обработку ПДн, назначенное приказом директора НКО:

(1) на этапе разработки и согласования типовых форм договоров, согласий Субъектов ПДн и пр.;

(2) в оперативном\текущем режиме – в момент визирования\подписания заключаемых договоров, содержащих ПДн Субъектов;

(3) в случаях поступления сведений об имеющихся нарушениях при осуществлении НКО обработки ПДн;

(4) по поручению директора\Совета директоров НКО;

(5) в иных случаях.

В случаях, указанных в подпунктах 3-5, могут создаваться возглавляемые Ответственным лицом специальные комиссии.

10.2. В рамках системы ВК могут проводиться ответственным лицом, СВА, СВК периодические (в т.ч. точечные) проверки, темами которых могут являться:

***10.2.1. при обработке ПДн без использования средств автоматизации:***

(1) хранение бумажных носителей, содержащих ПДн;

(2) доступ к бумажным носителям, содержащим ПДн;

(3) доступ в помещения, где обрабатываются и хранятся бумажные носители, содержащие ПДн;

(4) другие темы\вопросы.

***10.2.2. при обработке ПДн с использованием средств автоматизированной обработки персональных данных:***

(1) соответствие полномочий пользователя матрице доступа;

(2) соблюдение пользователями информационных систем персональных данных (далее – ИСПДн) требований парольной политики НКО;

(3) соблюдение пользователями ИСПДн антивирусной политики;

(4) соблюдение пользователями ИСПДн правил работы со съемными носителями ПДн;

(5) соблюдение ответственными за криптографические средства защиты информации правил работы с ними;

(6) соблюдение порядка доступа в помещения НКО, в которых расположены элементы ИСПДн;

(7) соблюдение порядка резервирования баз данных и хранения резервных копий;

(8) соблюдение порядка работы со средствами защиты информации;

(9) знание пользователями ИСПДн правил\инструкций своих действий во внештатных ситуациях;

(10) другие вопросы;

10.3. Проверки осуществляются непосредственно на месте обработки персональных данных посредством:

(1) опроса сотрудников,

(2) осмотра рабочих мест сотрудников, участвующих в процессе обработки ПДн,

(3) иных форм в соответствии с действующим законодательством.

10.4. По результатам проверки составляется Акт, в котором отражаются выявленные нарушения\недостатки и меры, необходимые и достаточные для их устранения.

Результаты устранения нарушений\недостатков (причины их неустранения в установленные сроки) доводятся до сведения директора НКО.

С Актом должны быть ознакомлены все задействованные в процессе проверки лица, подтверждением чего являются их собственноручные подписи.

10.5. Акты проверок хранятся у Ответственного лица, их уничтожение обеспечивается Ответственным лицом самостоятельно.

10.6. В рамках системы внутреннего контроля не реже одного раза в три года СВА осуществляет плановые и внеплановые проверки организации и функционирования в НКО системы обработки персональных данных.

**11. ПОРЯДОК ОЦЕНКИ УРОВНЯ\СТЕПЕНИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПДн В СЛУЧАЕ НАРУШЕНИЯ ФЕДЕРАЛЬНОГО ЗАКОНА "О ПЕРСОНАЛЬНЫХ ДАННЫХ"**

11.1. Оценка уровня\степени вреда, который может быть причинен Субъектам ПДн в случае нарушения Федерального закона [от 27 июля 2006 г. N 152-ФЗ](https://normativ.kontur.ru/document?moduleid=1&documentid=430502#l0) "О персональных данных" (далее – оценка вреда), обеспечивается ответственным(и) за организацию обработки ПДн в НКО, назначенным(и) приказом директора, не реже одного раза в год, а также при выявлении новых критериев возможного причинения вреда.

11.2. Степень вреда, который может быть причинен субъекту ПДн в случае нарушения [Закона](https://normativ.kontur.ru/document?moduleid=1&documentid=430502#l0) «О персональных данных», классифицируется в три категории – **высокая, средняя, низкая**:

|  |  |  |
| --- | --- | --- |
| **Критерии уровня\степени вреда** | **Наличие критериев** | **Степень \ уровень вреда** |
| 1. обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (***биометрические персональные данные***) и которые используются оператором для установления личности субъекта ПДн, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных | **🞏 - да**  **🞏 - нет** | **ВЫСОКАЯ**  **(выявлен хотя бы один из перечисленных факторов)** |
| 1. обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий ПДн | **🞏 - да**  **🞏 - нет** |
| 1. обработка ПДн несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации | **🞏 - да**  **🞏 - нет** |
| 1. обезличивание ПДн, в т. ч. с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований, не предусмотренных [пунктом 9](https://normativ.kontur.ru/document?moduleid=1&documentid=430502#l249) части 1 статьи 6 Закона о персональных данных | **🞏 - да**  **🞏 - нет** |
| 1. поручение иностранному лицу (иностранным лицам) осуществлять обработку ПДн граждан Российской Федерации | **🞏 - да**  **🞏 - нет** |
| 1. сбор ПДн с использованием баз данных, находящихся за пределами РФ | **🞏 - да**  **🞏 - нет** |
| 1. распространение ПДн на официальном сайте в информационно-телекоммуникационной сети "Интернет" оператора, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных | **🞏 - да**  **🞏 - нет** | **СРЕДНЯЯ**  **(выявлен хотя бы один из перечисленных факторов)** |
| 1. обработка ПДн в дополнительных целях, отличных от первоначальной цели сбора | **🞏 - да**  **🞏 - нет** |
| 1. продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз ПДн, владельцем которых является иной оператор | **🞏 - да**  **🞏 - нет** |
| 1. получение согласия на обработку ПДн посредством реализации на официальном сайте в информационно-телекоммуникационной сети "Интернет" функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта ПДн | **🞏 - да**  **🞏 - нет** |
| 1. осуществление деятельности по обработке ПДн, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять их обработку определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой | **🞏 - да**  **🞏 - нет** |
| 1. ведение общедоступных источников ПДн, сформированных в соответствии со статьей 8**\*** Закона о персональных данных   **\*** ***Статья 8. Общедоступные источники персональных данных***  *1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.*  *2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных* *органов*. | **🞏 - да**  **🞏 - нет** | **НИЗКАЯ** |
| 1. назначение в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником НКО (оператора ПДн) | **🞏 - да**  **🞏 - нет** |

11.3. Если по результатам проведенной оценки установлено, что в рамках деятельности по обработке ПДн Субъекту может быть причинен вред различной степени тяжести (высокая\средняя\низкая), в качестве итоговой оценки принимается худшая из них**\*\***.

**\*\* *возможные комбинации оценок:***

***1. высокая → средняя → низкая} → высокая степень вреда***

***2. высокая → средняя} → высокая степень вреда***

***3. высокая → низкая} → высокая степень вреда***

***4. средняя → низкая} → средняя степень вреда***

11.4. В зависимости от присвоенной оценки степени вреда, который может быть причинен Субъекту ПДн в случае нарушения Федерального закона «О персональных данных», принимаются необходимые и достаточные меры по обеспечению соответствующего уровня защищенности информационной системы НКО, в том числе указанные в Приложении № 5 к настоящему Положению.

**12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

12.1. Настоящее Положение (с изменениями и дополнениями) вступает в действие с рабочего дня, следующего за днем его утверждения.

12.2. Лица, виновные в нарушении норм, регулирующих обработку ПДн и защиту обрабатываемых в НКО персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.