

Приложение № 2 к постановлению
администрации Новоусманского
муниципального района от 14.05.2014 г. № _847_

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
в администрации Новоусманского
муниципального района Воронежской области

с. Новая Усмань
2014 г.

Оглавление

1.	Общие положения.....	5
2.	Требования по обработке персональных данных.....	6
2.1.	Понятия и определения.....	6
2.2.	Принципы обработки персональных данных.....	7
2.3.	Цели обработки персональных данных.....	8
2.4.	Способы и правила обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации.....	9
2.4.1.	Правила обработки персональных данных без использования средств автоматизации.....	9
2.4.2.	Правила обработки персональных данных средствами автоматизации.....	9
2.4.3.	Правила исключительно автоматизированной обработки персональных данных.....	11
2.4.4.	Правила смешенной обработки персональных данных.....	11
2.4.5.	Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных.....	11
2.5.	Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных.....	12
2.5.1.	Правила обработки специальных категорий персональных данных.....	12
2.5.2.	Правила обработки биометрических персональных данных.....	13
2.5.3.	Правила обработки общедоступных персональных данных.....	13
2.6.	Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных.....	14
2.6.1.	Правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию.....	14
2.6.2.	Правила обработки персональных данных при трансграничной передаче персональных данных	14
2.6.3.	Правила работы с обезличенными данными.....	15
2.6.4.	Правила обработки персональных данных в целях политической агитации.....	15
2.7.	Необходимость обработки персональных данных.....	15
2.8.	Перечни персональных данных, используемые для решения задач и функций структурными подразделениями.....	15
2.9.	Правовое основание обработки персональных данных.....	15
2.9.1.	Определение законности целей обработки персональных данных.....	15
2.9.2.	Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных.....	16
2.9.3.	Заданные характеристики безопасности персональных данных.....	16
2.9.4.	Определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных.....	17
2.10.	Действия (операции) с персональными данными.....	17
2.10.1.	Осуществление сбора персональных данных.....	18

2.10.2.	Осуществление систематизации, накопления, уточнения и использования персональных данных	19
2.10.3.	Осуществление записи и извлечения персональных данных.....	19
2.10.4.	Осуществление передачи персональных данных.....	19
2.10.5.	Осуществление хранения персональных данных.....	20
2.10.6.	Осуществление блокирования персональных данных.....	20
2.10.7.	Осуществление обезличивания персональных данных.....	20
2.10.8.	Осуществление удаления и уничтожения персональных данных.....	20
2.11.	Круг субъектов, персональные данные которых подлежат обработке.....	21
2.12.	Перечни должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных.....	22
2.13.	Права и обязанности при обработке персональных данных.....	22
2.13.1.	Права и обязанности субъекта персональных данных.....	22
2.14.	Порядок взаимодействия с субъектами персональных данных и иными лицами.....	28
2.14.1.	Установленные сроки выполнения действий по защите прав субъектов персональных данных	29
2.14.2.	Требования по уведомлениям (предоставлению информации, разъяснениям) субъектов персональных данных и в иных случаях.....	30
2.14.3.	Лица, ответственные за организацию обработки персональных данных.....	32
2.14.4.	Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав.....	32
2.14.5.	Порядок реагирования на обращения субъектов персональных данных.....	33
2.14.6.	Порядок действий при обращениях субъектов персональных данных.....	33
2.14.7.	Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных.....	35
2.14.8.	Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных.....	35
2.15.	Согласие субъекта персональных данных на обработку его персональных данных.....	35
2.16.	Уведомление об обработке (о намерении осуществлять обработку) персональных данных.....	36
2.17.	Информационные системы персональных данных.....	37
2.17.1.	Критерии определения информационных систем персональных данных.....	38
2.17.2.	Наименование информационной системы персональных данных.....	38
2.17.3.	Цели создания или эксплуатации информационной системы персональных данных.....	38
2.17.4.	Параметры, характеризующие информационную систему персональных данных.....	38
2.18.	Перечень информационных систем персональных данных.....	39
2.19.	Требования к сотрудникам, осуществляющим доступ к персональным данным или их обработку.....	39
2.20.	Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных.....	40
3.	Конфиденциальность персональных данных.....	40
3.1.	Режим ограниченного доступа к персональным данным.....	40

3.2.	Порядок учета и маркирования материальных носителей информации, образующихся в процессе обработки персональных данных.....	41
4.	Обеспечение безопасности персональных данных при их обработке.....	41
4.1.	Принципы обеспечения безопасности персональных данных при их обработке.....	41
4.2.	Требования по уровню обеспечения безопасности.....	42
4.3.	Состав мероприятий по обеспечению безопасности персональных данных.....	42
4.3.1.	Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.....	42
4.3.2.	Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации.....	42
4.4.	Система защиты персональных данных.....	44
4.4.1.	Частная модель угроз.....	45
4.4.2.	Средства защиты информации.....	45
4.5.	Требования к помещениям, в которых производится обработка персональных данных.....	46
4.6.	Порядок оценки соответствия требованиям по безопасности персональных данных.....	46
5.	Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных.....	46
5.1.	Порядок внешнего контроля над соблюдением требований по обработке и обеспечению безопасности данных.....	46
5.2.	Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных.....	47
5.3.	Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных.....	48
6.	Ответственность за нарушение требований в области персональных данных.....	49
7.	Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор).....	49
8.	Мероприятия по обработке персональных данных при проведении процедур ликвидации или реорганизации.....	49
9.	Ознакомление субъектов персональных данных с документами, определяющими политику в отношении обработки персональных данных.....	49
10.	Руководящие документы, используемые в настоящем Положении.....	50

1. Общие положения

Настоящее Положение обработки персональных данных В Организации (далее – Правила) разработано на основании и во исполнение:

- Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановления Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

и определяют **политику администрации Новоусманского муниципального района Воронежской области в отношении обработки персональных данных.**

Настоящее Положение утверждается и вводится в действие Распоряжением главы администрации Новоусманского муниципального района Воронежской области (далее – Руководитель) и являются обязательными для исполнения всеми сотрудниками администрации Новоусманского муниципального района Воронежской области (далее – Организация).

Настоящее Положение:

- устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- определяют для **каждой** цели обработки персональных данных:
 - содержание обрабатываемых персональных данных,
 - категории субъектов, персональные данные которых обрабатываются,
 - сроки их обработки и хранения,
 - порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
 - перечни персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций;
 - оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- определяют соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- устанавливают правила рассмотрения запросов субъектов персональных данных или их представителей;
- устанавливают правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;
- устанавливают типовую форму согласия на обработку персональных данных сотрудников и иных субъектов персональных данных;
- устанавливают типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- устанавливают правила работы с обезличенными данными;
- определяют перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- определяют перечень информационных систем персональных данных;
- определяют перечень должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- устанавливают порядок ознакомления сотрудников Организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных),

локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных сотрудников;

- устанавливают перечень и правила ведения иных локальных актов по вопросам обработки персональных данных, включая:

- порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;
- должностную инструкцию ответственного за организацию обработки персональных данных;
- типовое обязательство сотрудников, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ними государственного контракта (трудового договора) прекратить обработку персональных данных, ставших известными в связи с исполнением должностных обязанностей.

2. Требования по обработке персональных данных

2.1. Понятия и определения

В настоящем Положении используются следующие основные понятия:

- **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- **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;

- **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;

- **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **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** – 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;

- **конфиденциальность персональных данных** – обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

- **специальные категории персональных данных** – персональные данные, в том числе, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, о судимости;
- **биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность;
- **использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- **доступ к информации** – возможность получения информации и ее использования;
- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- **под техническими средствами**, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;
- **базой данных является** представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ);
- **к юридическим последствиям** относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

Иные понятия в настоящем Положении используются в значениях, определенных действующим законодательством Российской Федерации либо их значение дается по тексту.

2.2. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе следующих принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- обязанность лица, осуществляющего обработку персональных данных по поручению оператора, соблюдения принципов и правил обработки персональных данных;
- соблюдения принципов и правил обработки персональных данных при поручении такой обработки другому лицу;
- соблюдение конфиденциальности персональных данных;
- обработки персональных данных (в том числе при обработке общедоступных персональных данных, специальных категорий персональных данных, биометрических персональных данных, при принятии решений на основании исключительно автоматизированной обработки персональных данных, при трансграничной передаче персональных данных) с письменного согласия субъектов персональных данных либо на ином законном основании;
- соблюдения законности при осуществлении трансграничной передачи персональных данных;
- соблюдением обязанностей, возлагаемых на оператора персональных данных, действующим законодательством и иными нормативными актами по обработке персональных данных;
- принятии мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных;
- принятии необходимых правовых, организационных и технических мер или обеспечении их принятия 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;
- недопустимости ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных;
- недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку персональных данных;
- документального оформления всех принятых решений по обработке и обеспечению безопасности персональных данных.

Нарушение указанных принципов обработки персональных данных категорически запрещается!

2.3. Цели обработки персональных данных

Организация, являясь оператором персональных данных, должна определять цели обработки персональных данных в своих информационных системах персональных данных.

Цели обработки персональных данных в информационных системах персональных данных должны быть четко определены и соответствовать:

- заявленным в Положении основным полномочиям и правам Организации;
- перечням задач или функций структурных подразделений (должностных лиц) Организации, указанным в положениях о таких структурных подразделениях (должностных обязанностях).

Определение целей обработки персональных данных в информационных системах персональных данных производится в Правилах обработки персональных данных конкретных информационных систем персональных данных Организации (см. пункт 3.5 настоящего Положения).

Цели обработки персональных данных определяют:

- содержание и объем обрабатываемых персональных данных,
- категории субъектов, персональные данные которых обрабатываются,
- сроки их обработки и хранения,
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Цели обработки персональных данных должны быть:

- конкретны;
- заранее определены;
- законны;
- заявлены.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Совместимость целей определяется по наличию общей цели связанной с заявленными в Положении

основными полномочиями и правами Организации или по наличию общей цели, определяемой действующим законодательством Российской Федерации.

2.4. Способы и правила обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации

Способы обработки персональных данных в информационных системах персональных данных:

- обработка персональных данных без использования средств автоматизации;
- обработка персональных данных с использованием средств автоматизации;
- исключительно автоматизированная обработка персональных данных;
- смешанная обработка персональных данных.

2.4.1. Правила обработки персональных данных без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности, при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных, осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:
 - сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации,
 - имя (наименование) и адрес оператора,
 - фамилию, имя, отчество и адрес субъекта персональных данных,
 - источник получения персональных данных,
 - сроки обработки персональных данных,
 - перечень действий с персональными данными, которые будут совершаться в процессе их обработки,
 - общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых, заведомо не совместимы.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится 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.

2.4.2. Правила обработки персональных данных средствами автоматизации

Обработка персональных данных средствами автоматизации в Организации допускается только в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных законом, для

осуществления и выполнения возложенных законодательством Российской Федерации на Организацию функций, полномочий и обязанностей;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов Организации или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка персональных данных средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащих такие данные, определенные для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящего Положения.

2.4.2.1. Обработка персональных данных с согласия субъекта персональных данных

В случае если обработка персональных данных субъекта персональных данных в информационной системе персональных данных осуществляется на основании согласия и не имеется оснований для обработки таких персональных данных без получения согласия, должны выполняться указанные в настоящем пункте положения.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных должно быть:

- конкретным,
- информированным,
- сознательным.

Согласие на обработку персональных данных Организации может быть дано субъектом персональных данных или его представителем только в письменной форме. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

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

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

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны представить документы, подтверждающие их полномочия.

Допускается включение согласия в типовые формы (бланки) материальных носителей персональных

данных и в договоры с субъектами персональных данных.

Письменные согласия субъектов персональных данных должны храниться в Организации.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем направления обращения в Организацию. При получении такого обращения выполняются действия предусмотренные пунктом 2.14.8 настоящего Положения.

Требования к содержанию согласия на обработку персональных данных приведено в пункте 2.15 настоящего Положения.

2.4.2.2. Обработка персональных данных без согласия субъекта персональных данных

Обработка персональных данных, осуществляемая без получения согласия на такую обработку от субъекта персональных данных может осуществляться только по основаниям, указанным в пункте 2.4.2, при этом обязанность предоставить доказательство наличия таких оснований возлагается на Организацию.

Порядок определения оснований обработки персональных данных без согласия на обработку персональных данных от субъекта персональных данных, их определения, оформления и предоставления приведен в пунктах 2.7, 2.9 и 2.14 настоящего Положения.

2.4.3. Правила исключительно автоматизированной обработки персональных данных

При исключительно автоматизированной обработке персональных данных должны выполняться правила обработки персональных данных средствами автоматизации (пункт 2.4.2 настоящего Положения).

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

В остальных случаях принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы запрещается.

При исключительно автоматизированной обработке персональных данных необходимо:

- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных;
- разъяснить возможные юридические последствия такого решения;
- предоставить возможность заявить возражение против такого решения;
- рассмотреть возражение;
- уведомить субъекта персональных данных о результатах рассмотрения такого возражения в порядке определенном в пункте 2.14.2 настоящего Положения в сроки, предусмотренные пунктом 2.14.1 настоящего Положения.

2.4.4. Правила смешанной обработки персональных данных

При смешанной обработке персональных данных необходимо выполнять правила объединяющие правила обработки персональных данных при их обработке каждым из используемых при смешанной обработке персональных данных способов (пункты 2.4.1-2.4.3 настоящего Положения).

2.4.5. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных

2.4.5.1. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных другому лицу

Организация вправе поручить обработку персональных данных другому лицу (поручение оператора):

- с согласия субъекта персональных данных;
- если иное не предусмотрено федеральным законом;
- на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта;
- либо путем принятия соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Положением.

В поручении оператора:

- должен быть определен перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- должны быть определены цели обработки персональных данных;
- должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных;
- должна быть установлена обязанность такого лица обеспечивать безопасность персональных данных при

их обработке;

- должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с настоящим Положением и техническим заданием на создание системы защиты персональных данных;
- установлена ответственность такого лица перед Организацией, в случаях нарушений установленных требований и законодательства Российской Федерации в области персональных данных;
- при необходимости получения согласий на обработку персональных данных от субъектов персональных данных, предусмотрен порядок сбора и передачи в Организацию таких согласий субъектов персональных данных.

В случае если Организация поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет непосредственно сама Организация.

В случае необходимости получения согласия на обработку персональных данных от субъекта персональных данных обязанность получения таких согласий возлагается на Организацию.

2.4.5.2. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных другим лицом

В случае поручения обработки персональных данных средствами автоматизации Организацией другим лицом, такое лицо своим поручением оператору обязано:

- определить перечень действий (операций) с персональными данными, которые будут совершаться Организацией при осуществлении обработки персональных данных;
- определить цели обработки персональных данных;
- указать требования к защите обрабатываемых персональных данных.

В случае не определения такой информации и требований другим лицом, Организация обязана добиться их определения и документального оформления.

В случае принятия поручения оператора от другого лица Организацией без указанной информации и требований, такая обработка не считается обработкой осуществляемой по поручению оператора, Организация будет являться оператором персональных данных. При этом обработка персональных данных должна выполняться в соответствии с настоящим Положением за исключением пункта 2.4.5.

Организация обязана выполнить все требования установленные другим лицом в поручении оператора и за все нарушения в обработке персональных данных несет ответственность перед таким лицом.

Организация при осуществлении обработки персональных данных по поручению оператора не обязана получать согласие субъекта персональных данных на обработку его персональных данных.

2.5. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных

В Организации устанавливаются следующие особые правила обработки персональных данных в зависимости от категории обрабатываемых персональных данных:

- обработка специальных категорий персональных данных;
- обработка общедоступных персональных данных.

Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных являются дополнительными способами и правилами обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации указанным в пункте 2.4 настоящего Положения.

2.5.1. Правила обработки специальных категорий персональных данных

К специальным категориям персональных данных относятся сведения касающиеся:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- состояния здоровья;
- интимной жизни;
- судимости.

В Организации **категорически запрещается** обработка специальных категорий персональных данных касающихся:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- интимной жизни.

В Организации разрешается обработка сведений специальных категорий персональных данных

касающиеся состоянию здоровья и судимости в минимально необходимом объеме при обязательном соблюдении любого из следующих условий:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, о противодействии терроризму, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка персональных данных о судимости осуществляется в пределах полномочий, предоставленных Организации в соответствии с законодательством Российской Федерации.

Обработка специальных категорий персональных данных в остальных случаях в Организации не допускается.

Обработка специальных категорий персональных данных, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

2.5.2. Правила обработки биометрических персональных данных

К биометрическим персональным данным относятся сведения (обязательно выполнение всех трех условий одновременно), характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность.

Обработка биометрических персональных данных в Организации **запрещена**.

2.5.3. Правила обработки общедоступных персональных данных

Общедоступные персональные данные физических лиц, полученные из сторонних общедоступных источников персональных данных, в Организации обрабатываются в исключительных случаях в сроки, не превышающие необходимых для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта персональных данных на включение такой информации в общедоступные источники персональных данных, так как в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на Организацию. По достижении целей обработки общедоступных персональных данных они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия как внутри Организации, так и со сторонними физическими и юридическими лицами в Организации могут создаваться общедоступные источники персональных данных. Создание общедоступного источника персональных данных осуществляется по решению Руководителя. В решении о создании общедоступного источника персональных данных должны быть указаны:

- цель создания общедоступного источника персональных данных;
- ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника персональных данных (при наличии);
- перечень персональных данных, которые вносятся в общедоступный источник персональных данных;
- порядок включения персональных данных в общедоступный источник персональных данных;
- порядок уведомления пользователей общедоступного источника персональных данных об исключении из него персональных данных либо внесении в него изменений;
- порядок получения письменного согласия субъекта персональных данных на включение персональных данных в общедоступный источник персональных данных;
- ссылка на нормативный акт, устанавливающий порядок исключения персональных данных из общедоступного источника персональных данных.

В общедоступный источник персональных данных с письменного согласия субъекта персональных данных могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники персональных данных персональных данных

субъекта персональных данных допускается только на основании его письменного согласия.

Исключение персональных данных из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта персональных данных в установленном настоящим Положением (пункт 2.14.8) и действующим законодательством Российской Федерации порядке.

2.6. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных

В Организации устанавливаются следующие особые правила обработки персональных данных в зависимости от цели обработки персональных данных:

- правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию;
- правила обработки персональных данных при трансграничной передаче персональных данных;
- правила работы с обезличенными данными;
- правила обработки персональных данных в целях политической агитации.

Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных являются дополнительными способом и правилам обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации указанным в пункте 2.4 настоящего Положения.

2.6.1. Правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Организации, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Организации, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (по должностям), имеющих доступ к материальным носителям и перечень лиц, ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Организация, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на охраняемую территорию.

2.6.2. Правила обработки персональных данных при трансграничной передаче персональных данных

Трансграничной передачей персональных данных называется передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Трансграничной передачи персональных данных Организацией не осуществляется.

В случае принятия Организацией решения о трансграничной передаче персональных данных, такие данные могут обрабатываться только в следующих случаях:

- при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- предусмотренных международными договорами Российской Федерации;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Организация до начала осуществления трансграничной передачи персональных данных обязана убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

2.6.3. Правила работы с обезличенными данными

Обезличиванием персональных данных называются действия, в результате которых становится

невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Порядок обезличивания в Организации установлен пунктом 2.10.7 настоящего Положения.

2.6.4. Правила обработки персональных данных в целях политической агитации

Организация не осуществляет обработки персональных данных в целях политической агитации.

В случае принятия Организацией решения об обработке персональных данных в целях политической агитации, такая обработка может осуществляться только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если Организация не докажет, что такое согласие было получено.

Организация по требованию субъекта персональных данных обязана немедленно прекратить обработку его персональных данных, осуществляемую в целях политической агитации.

2.7. Необходимость обработки персональных данных

Необходимость обработки персональных данных определяется заранее определенной и документированной целью обработки персональных данных и может устанавливаться (требоваться) нормативно-правовым актом (например, федеральным законом) или определяется принятым в Организации порядком выполнения определенных операций по обработке информации, в рамках заявленных в Положении основных полномочий и прав, либо в рамках перечня задач или функций структурных подразделений (должностных лиц), указанных в положениях о таких структурных подразделениях (должностных обязанностях).

Принятый в Организации порядок выполнения определенных операций по обработке информации, в рамках которых производится обработка персональных данных, должен быть отражен в локальном нормативном акте.

Обработка персональных данных без определения правового основания ее необходимости **категорически запрещается.**

2.8. Перечни персональных данных, используемые для решения задач и функций структурными подразделениями

Для решения тех или иных задач и функций структурными подразделениями Организации определяются наборы персональных данных, обработка которых вызвана заранее определенной и документированной целью обработки персональных данных.

Обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных недопустима.

Перечни персональных данных, используемых для решения конкретных задач и функций структурными подразделениями в Организации оформляются в порядке, установленном пунктом 2.18 настоящего Положения.

2.9. Правовое основание обработки персональных данных

Правовое основание обработки персональных данных включает в себя:

- определение законности целей обработки персональных данных;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- определение заданных характеристик безопасности персональных данных;
- определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных.

2.9.1. Определение законности целей обработки персональных данных

Заявляемые в качестве целей обработки персональных данных цели должны быть законны. Законность целей обработки персональных данных в Организации определяется их соответствием случаям, указанным в пункте 2.4.2 настоящего Положения.

Причем, кроме самого факта обработки персональных данных, должны рассматриваться и, соответственно, иметь правовое основание, особые правила обработки определенных наборов персональных данных (таких как специальные категории персональных данных, биометрические персональные данные и др.), особые способы обработки персональных данных (обработка без использования средств автоматизации, исключительно автоматизированная обработка персональных данных и др.), а так же особые цели обработки персональных данных (однократный пропуск на охраняемую территорию, трансграничная передача персональных данных и др.).

При определении правовых оснований обработки персональных данных должны определяться реквизиты федерального закона, а также иных подзаконных актов, и документов органов государственной власти, которые требуют обработку персональных данных или иных документов, являющихся такими

основаниями.

Обработка персональных данных без документально определенного и оформленного правового основания обработки персональных данных не допускается.

2.9.2. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных при выполнении заявленных в Положении основных полномочий и прав Организации, либо в рамках перечня задач или функций структурных подразделений (должностных лиц), указанных в положениях о таких структурных подразделениях (должностных обязанностях) с учетом особых правил и способов обработки персональных данных.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

Обработка персональных данных без оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных не допускается.

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных документально оформляется установленным порядком.

2.9.3. Заданные характеристики безопасности персональных данных

Всеми лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность персональных данных – это обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Вне зависимости от необходимости обеспечения конфиденциальности персональных данных, при обработке персональных данных должно определяться наличие требований по обеспечению иных характеристик безопасности персональных данных, отличных от нее.

К таким характеристикам относятся:

- требование по обеспечению защищенности от уничтожения персональных данных;
- требование по обеспечению защищенности от изменения персональных данных;
- требование по обеспечению защищенности от блокирования персональных данных;
- требование по обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности персональных данных может устанавливаться:

- федеральным законом, а также иным подзаконным актом, документом органов государственной власти;
- актом Организации.

При определении необходимости обеспечения характеристик безопасности персональных данных, отличных от конфиденциальности, актом Организации, основным критерием должна служить оценка вреда, который может быть причинен субъектам персональных данных, с чьими персональными данными произошло нарушение таких характеристик безопасности персональных данных.

При принятии Организацией решения на обеспечение характеристик безопасности персональных данных, отличных от конфиденциальности, оно должно быть определено и документально оформлено.

Обработка персональных данных без документально определенного и оформленного решения по определению характеристик безопасности персональных данных не допускается.

2.9.4. Определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных

На основании определенных целей обработки персональных данных, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки персональных данных, в том числе хранения.

Указанные сроки должны быть определены и документально оформлены.

Определение сроков хранения осуществляется в соответствии с требованиями архивного законодательства Российской Федерации, в том числе, в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих персональные данные, в различных целях, определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку. При этом в случае наличия персональных данных в таких документах, обработка которых более не требуется, производится действия по уничтожению таких данных в порядке, определяемым пунктом 2.10 настоящего Положения.

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов и оформляется договором между Организацией и государственным или муниципальным архивом. При этом объем передаваемых документов и условия передачи определяется условиями такого договора и действующим требованиями архивного законодательства Российской Федерации.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящего Положения не распространяется.

Обработка персональных данных без документально определенных и оформленных сроков обработки, в том числе хранения персональных данных не допускается.

С целью выполнения требования по уничтожению либо обезличиванию персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, в Организации создается комиссия, определяющая факт достижения целей обработки персональных данных и достижение предельных сроков хранения документов, содержащих персональные данные. Порядок работы данной комиссии устанавливается отдельным Положением. Правила, устанавливаемые таким Положением, не должны противоречить настоящему Положению.

2.10. Действия (операции) с персональными данными

Обработкой персональных данных называется любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая:

- сбор персональных данных,
- запись персональных данных,
- систематизацию персональных данных,
- накопление персональных данных,
- хранение персональных данных,
- уточнение (обновление) персональных данных,
- уточнение (изменение) персональных данных,
- извлечение персональных данных,
- использование персональных данных,
- передачу (распространение) персональных данных,
- передачу (предоставление) персональных данных,
- передачу (доступ) персональных данных,
- обезличивание персональных данных,
- блокирование персональных данных,
- удаление персональных данных,
- уничтожение персональных данных.

Указанные действия (операции) с персональными данными в информационных системах персональных данных должны быть определены и документально оформлены в порядке, установленным настоящим Положением. При документальном оформлении действий (операций) с персональными данными рекомендуется использовать только указанные термины.

Обработка персональных данных без определенных и документально оформленных действий (операций) совершаемых с персональными данными не допускается.

2.10.1. Осуществление сбора персональных данных

2.10.1.1. Способы сбора персональных данных и источники их получения

В Организации применяются следующие способы получения персональных данных субъектов персональных данных:

- заполнение субъектом персональных данных соответствующих форм (в том числе для заключения договора);
 - получение персональных данных от третьих лиц;
 - получение данных на основании запроса третьим лицам;
 - сбор данных из общедоступных источников.
- Получение персональных данных в Организации допускается только:
- непосредственно от субъекта персональных данных;
 - из общедоступных источников;
 - от третьих лиц по основаниям, указанным в пункте 2.4.2 настоящего Положения.
- Получение персональных данных из иных источников не допускается.

В связи с необходимостью постоянного контроля за наличием персональных данных в общедоступных источниках персональных данных, получение и использование таких данных является не рекомендуемым и должно осуществляться только в исключительных случаях в сроки, не превышающие необходимых для принятия соответствующего решения.

2.10.1.2. Правила сбора персональных данных

При сборе персональных данных Организация обязана предоставить субъекту персональных данных по его просьбе информацию, предусмотренную пунктом 2.14.6.3 настоящего Положения.

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Организация обязана разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные (пункт 2.9.1 настоящего Положения).

Если основания на обработку персональных данных без согласия отсутствуют, то необходимо получение согласия субъекта персональных данных на обработку его персональных данных в соответствии с пунктом 2.15 настоящего Положения. Обработка персональных данных без получения такого согласия категорически запрещается.

Сбор персональных данных должен осуществляться с учетом правил и особых правил обработки персональных данных, предусмотренных пунктами 2.4-2.9 настоящего Положения.

Если персональные данные получены не от субъекта персональных данных, Организация до начала обработки таких персональных данных обязана предоставить субъекту персональных данных (в соответствии с 2.14.2 настоящего Положения) следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные права субъекта персональных данных;
- источник получения персональных данных.

Организация освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены Организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- Организация осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных сведений, которые Организация обязана предоставить субъекту персональных данных до начала обработки таких персональных данных если персональные данные получены не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

2.10.2. Осуществление систематизации, накопления, уточнения и использования персональных данных

Систематизация, накопление, уточнение, использование персональных данных могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

В Организации могут быть установлены особенности учета персональных данных в информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей информационной системе персональных данных, конкретному субъекту персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с

использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных.

Уточнение персональных данных должно производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении персональных данных субъекта персональных данных принимается лицом, ответственным за организацию обработки персональных данных в Организации.

Использование персональных данных должно осуществляться исключительно в заявленных целях. Использование персональных данных в заранее не определенных и не оформленных установленным образом целях категорически не допускается.

2.10.3. Осуществление записи и извлечения персональных данных

Запись персональных данных в информационные системы персональных данных Организации может осуществляться с любых носителей информации или из других информационных систем персональных данных.

Извлечение персональных данных из информационных систем персональных данных может осуществляться с целью:

- вывода персональных данных на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;
- вывода персональных данных на носители информации, предназначенные для их обработки средствами вычислительной техники.

При извлечении персональных данных должен проводиться учет носителей информации.

При осуществлении записи и извлечения персональных данных должны соблюдаться условия обработки персональных данных, конфиденциальность персональных данных и иные требования, указанные в настоящем Положении.

2.10.4. Осуществление передачи персональных данных

Передача персональных данных в Организации должна осуществляться с соблюдением настоящего Положения и действующего законодательства Российской Федерации.

В Организации приняты следующие способы передачи персональных данных субъектов персональных данных:

- передача персональных данных на электронных носителях информации посредством нарочного;
- передача персональных данных на бумажных носителях посредством нарочного;
- передача персональных данных на электронных носителях посредством почтовой связи;
- передача персональных данных на бумажных носителях посредством почтовой связи;
- передача персональных данных по каналам электрической связи.

Перед осуществлением передачи персональных данных проверяется основание на осуществление такой передачи и наличие согласия на передачу персональных данных в согласии субъекта персональных данных на обработку персональных данных или наличие иных законных оснований, предусмотренных пунктом 2.4.2 настоящего Положения.

Передача персональных данных должна осуществляться на основании:

- договора с третьей стороной, которой осуществляется передача персональных данных;
- запроса, полученного от третьей стороны, которой осуществляется передача персональных данных;
- исполнения возложенных законодательством Российской Федерации на Организацию функций, полномочий и обязанностей.

Передача персональных данных без согласия или иных законных оснований категорически запрещается.

Передача персональных данных должна осуществляться с учетом правил и особых правил обработки персональных данных, предусмотренных пунктами 2.4-2.9 настоящего Положения.

2.10.5. Осуществление хранения персональных данных

Хранение персональных данных в Организации допускается только в форме документов – зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

- изобразительный документ – документ, содержащий информацию, выраженную посредством изображения какого-либо объекта
- фотодокумент – изобразительный документ, созданный фотографическим способом;
- текстовый документ – документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

- письменный документ – текстовый документ, информация которого зафиксирована любым типом письма;
- рукописный документ – письменный документ, при создании которого знаки письма наносят от руки;
- машинописный документ – письменный документ, при создании которого знаки письма наносят техническими средствами;
- документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение персональных данных в Организации осуществляется в форме, позволяющей определить субъект персональных данных не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого выгодоприобретателем или поручителем по которому является субъект персональных данных.

Хранение персональных данных в информационных системах персональных данных Организации и вне таких систем осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного:

- доступа к ним,
- их уничтожения,
- изменения,
- блокирования,
- копирования,
- предоставления,
- распространения.

2.10.6. Осуществление блокирования персональных данных

Блокированием персональных данных называется временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Блокирование персональных данных конкретного субъекта персональных данных должно осуществляться во всех информационных системах персональных данных Организации, включая архивы баз данных, содержащих такие персональные данные, информационных систем персональных данных.

Блокирование персональных данных в Организации осуществляется:

- в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;
- в случае отсутствия возможности уничтожения персональных данных в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки персональных данных Организация осуществляет снятие блокирования персональных данных.

Решение о блокировании и снятии блокирования персональных данных субъекта персональных данных принимается ответственным за организацию обработки персональных данных в Организации.

2.10.7. Осуществление обезличивания персональных данных

Обезличивание персональных данных в Организации при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей.

Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.10.8. Осуществление удаления и уничтожения персональных данных

Уничтожение персональных данных это 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.

Уничтожение персональных данных в Организации производится только в следующих случаях:

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки персональных данных, если обеспечить

правомерность обработки персональных данных невозможно;

- в случае достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных.

По факту уничтожения персональных данных обязательно проверяется необходимость уведомления об этом и в случае наличия такого требования, осуществляется уведомление указанных в таком требовании лиц, в порядке, приведенном в пункте 2.14.2 настоящего Положения.

При уничтожении персональных данных необходимо:

- убедиться в необходимости уничтожения персональных данных;
- убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;
- уничтожить персональные данные подходящим способом, в соответствии с настоящим Положением или способом, указанным в соответствующем требовании или распорядительном документе;
- проверить необходимость уведомления об уничтожении персональных данных;
- при необходимости, уведомить об уничтожении персональных данных требуемых лиц.

При уничтожении персональных данных применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) – для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержащем персональные данные;
- измельчение в специальной бумагорезательной (бумагоуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для носителей информации на оптических дисках;
- физическое уничтожение частей носителей информации – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении персональных данных необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части персональных данных допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение персональных данных производится лицами, обрабатывающими персональные данные в соответствующей информационной системе персональных данных, в которой производится уничтожение персональных данных, только в присутствии лица, ответственного за организацию обработки персональных данных в Организации.

По факту уничтожения персональных данных составляется Акт уничтожения персональных данных, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки персональных данных Организации, присутствовавшим при уничтожении и утверждается Руководителем.

Хранение актов уничтожения персональных данных осуществляется в течение срока исковой давности, если иное не установлено нормативно-правовыми актами Российской Федерации.

2.11. Круг субъектов, персональные данные которых подлежат обработке

Круг субъектов, персональные данные которых подлежат обработке в информационных системах персональных данных Организации, определяется целью обработки персональных данных в каждой информационной системе персональных данных.

2.12. Перечни должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных

Лицо, ответственное за организацию обработки персональных данных В Организации готовит и уточняет:

- перечень должностей сотрудников Организации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, в котором указываются должности сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным для каждой информационной системы персональных данных, а также уровень полномочий в них;
- перечень должностей сотрудников Организации, ответственных за проведение мероприятий по

обезличиванию обрабатываемых персональных данных.

Указанные перечни должностей сотрудников в Организации подписываются лицом, ответственным за организацию обработки персональных данных и утверждаются Руководителем.

2.13. Права и обязанности при обработке персональных данных

2.13.1. Права и обязанности субъекта персональных данных

2.13.1.1. Права субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в Организации, имеет право:

- на получение сведений о подтверждении факта обработки персональных данных Организацией;
- на получение сведений о правовых основаниях и цели обработки персональных данных;
- на получение сведений о цели и применяемых Организацией способов обработки персональных данных;
- на получение сведений о наименовании и месте нахождения Организации, сведений о лицах (за исключением сведений о сотрудниках Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Организацией или на основании федерального закона;
- на получение сведений об обрабатываемых персональных данных, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- на получение сведений о сроках обработки персональных данных, в том числе сроках их хранения;
- на получение сведений о порядке осуществления субъектом персональных данных своих прав, предусмотренных законодательством в области персональных данных;
- на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;
- на получение сведений о наименовании и адресе лица, осуществляющего обработку персональных данных по поручению Организации, если обработка поручена или будет поручена такому лицу;
- на получение иных сведений, предусмотренных законодательством в области персональных данных и другими федеральными законами;
- требовать от Организации 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;
- принимать предусмотренные законом меры по защите своих прав;
- требовать от Организации предоставления ему персональных данных в доступной форме;
- повторного обращения и запроса в целях получения сведений и ознакомления с его персональными данными;
- требовать разъяснения порядка принятия решения на основании исключительно автоматизированной обработки его персональных данных;
- заявить возражение против принятия решения на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы;
- требовать разъяснения порядка принятия и возможные юридические последствия принятия решения на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, а также разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;
- обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- требовать предоставления безвозмездно субъекту персональных данных или его представителю возможности ознакомления с персональными данными, относящимися к этому субъекту персональных данных;
- принимать решение о предоставлении его персональных данных и давать согласие на их обработку свободно, своей волей и в своем интересе;
- отзываться согласие на обработку персональных данных.

Кроме указанных прав в вопросах обработки его персональных данных субъект персональных данных обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

2.13.1.2. Обязанности субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в Организации, обязан:

- предоставлять свои персональные данные в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных;
- с целью соблюдения его законных прав и интересов подавать только достоверные персональные данные.

Кроме указанных обязанностей в вопросах обработки его персональных данных на субъекта персональных данных налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

2.13.1.3. Права и обязанности Организации при обработке персональных данных субъектов персональных данных

2.13.1.4. Права Организации при обработке персональных данных субъектов персональных данных

Организация при обработке персональных данных субъектов персональных данных имеет право:

- обрабатывать персональные данные в соответствии с пунктом 2.4.2 настоящего Положения;
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта;
- мотивированно отказать субъекту персональных данных в выполнении повторного запроса в целях получения сведений касающейся обработки его персональных данных, при нарушении субъектом персональных данных своих обязанностей по подаче такого запроса;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором или Организацией;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если персональные данные получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если предоставление субъекту персональных данных таких сведений, нарушает права и законные интересы третьих лиц;
- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных, если иное не предусмотрено указанным законом и другими федеральными законами;
- если обеспечить правомерность обработки персональных данных невозможно, осуществлять или обеспечивать осуществление блокирования или уничтожения персональных данных в сроки, указанные в пункте 2.14.1 настоящего Положения;
- в случае достижения цели обработки персональных данных осуществлять или обеспечивать осуществление уничтожения персональных данных в сроки, указанные в пункте 2.14.1 настоящего Положения;
- в случае достижения цели обработки персональных данных продолжить обработку персональных данных, если это предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и субъектом персональных данных;
- в случае достижения цели обработки персональных данных продолжить обработку персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных

- на основаниях, предусмотренных пунктом 2.4.2 настоящего Положения или федеральными законами;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных продолжить обработку персональных данных, если это предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и субъектом персональных данных;
 - в случае отзыва субъектом персональных данных согласия на обработку его персональных данных продолжить обработку персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных пунктом 2.4.2 настоящего Положения или федеральными законами;
 - в случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пункте 2.14.1 настоящего Положения, осуществить блокирование таких персональных данных и обеспечить уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;
 - осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, указанных в пункте 2.16 настоящего Положения.
- Кроме указанных прав в вопросах обработки персональных данных субъектов персональных данных Организация обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

2.13.1.5. Обязанности Организации при обработке персональных данных субъектов персональных данных

Организация при обработке персональных данных субъектов персональных данных обязана:

- строго соблюдать принципы обработки персональных данных, указанные в пункте 2.2 настоящего Положения;
- строго соблюдать правила обработки персональных данных, указанные в пункте 2.4-2.6 настоящего Положения;
- в случае если, обработка персональных данных осуществляется по поручению оператора, строго соблюдать и выполнять требования поручения оператора;
- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников персональных данных сведения о субъекте персональных данных;
- обеспечить конкретность и информированность согласия на обработку персональных данных;
- получать согласие на обработку персональных данных в форме, указанной в пункте 2.15 настоящего Положения;
- в случае получения согласия на обработку персональных данных от представителя субъекта персональных данных проверять полномочия данного представителя на дачу согласия от имени субъекта персональных данных;
- предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований обработки персональных данных без получения согласия;
- строго соблюдать требования, к содержанию согласия в письменной форме субъекта персональных данных на обработку его персональных данных в соответствии с пунктом 2.15 настоящего Положения;
- незамедлительно прекратить обработку специальных категорий персональных данных если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом;
- убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных;
- предоставить субъекту персональных данных сведения по запросу субъекта персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных;
- мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта персональных данных;
- доказывать, что от субъекта персональных данных было получено предварительное согласие на обработку персональных данных в целях политической агитации;
- немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в целях политической агитации;
- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические

последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;

- рассмотреть возражение против принятия решения на основании исключительно автоматизированной обработки его персональных данных в течение срока указанного в пункте 2.14.1 настоящего Положения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;
- предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных;
- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом
- до начала обработки персональных данных, полученных не от субъекта персональных данных, предоставить субъекту персональных данных информацию о своем наименовании и адресе, цели обработки персональных данных и ее правовом основании, предполагаемых пользователей персональных данных, установленные права субъекта персональных данных, источник получения персональных данных;
- принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области персональных данных, если иное не предусмотрено федеральными законами;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- по запросу уполномоченного органа по защите прав субъектов персональных данных представить документы и локальные акты, определяющие политику в отношении обработки персональных данных и сведения о реализуемых требованиях к защите 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;
- сообщить субъекту персональных данных 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 персональных данных или его представителя либо при получении запроса субъекта персональных данных или его представителя;
- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ;
- предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных
- внести в персональные данные необходимые изменения или уничтожить такие персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными;
- строго соблюдать сроки по уведомлениям, блокированию и уничтожению персональных данных в соответствии с пунктом 2.14.1 настоящего Положения;
- уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;
- сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию;
- в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;
- в случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан, осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

- уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снять блокирование персональных данных в случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов;
- прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора;
- уничтожить персональные данные или обеспечить их уничтожение в случае, если обеспечить правомерность обработки персональных данных невозможно;
- уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган об устранении допущенных нарушений или об уничтожении персональных данных;
- прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае достижения цели обработки персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных пунктом 2.4.2 настоящего Положения или федеральными законами;
- прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных пунктом 2.4.2 настоящего Положения или федеральными законами;
- уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных в соответствии с пунктом 2.16 настоящего Положения;
- уведомить уполномоченный орган по защите прав субъектов персональных данных в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку персональных данных;
- назначить лицо, ответственное за организацию обработки персональных данных;
- предоставлять лицу, ответственному за организацию обработки персональных данных, необходимые сведения, указанные в пункте 2.14.3 настоящего Положения;
- неукоснительно соблюдать все требования настоящего Положения;
- ознакомить сотрудников Организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) обучить таких сотрудников;

Кроме указанных обязанностей в вопросах обработки персональных данных субъектов персональных данных на Организацию налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

2.13.1.6. Меры, направленные на обеспечение выполнения оператором своих обязанностей

Организация принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных. Организация определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения указанных обязанностей, в том числе:

- назначает ответственного за организацию обработки персональных данных в Организации из числа сотрудников данного органа (пункт 2.14.3 настоящего Положения);
- разрабатывает и утверждает должностную инструкцию ответственного за организацию обработки персональных данных в государственном или муниципальном органе (пункт 2.14.3 настоящего Положения);
- создает комиссию, в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (пункт 4 настоящего Положения);
- издает и утверждает приказом Руководителя Положение по обработке персональных данных

(Настоящего Положения):

- Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.(пункт 2.13.2.4 настоящего Положения);
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (пункт 2.10.8 настоящего Положения);
- правила рассмотрения запросов субъектов персональных данных или их представителей (пункты 2.14.5-2.14.6 настоящего Положения);
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных и локальным актам Организации (пункт 4 настоящего Положения);
- правила работы с обезличенными данными (пункт 2.10.7 настоящего Положения);
- типовую форму согласия на обработку персональных данных субъектов персональных данных (пункт 2.16 настоящего Положения);
- типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (пункт 2.14.4 настоящего Положения);
- оценку вреда, который может быть причинен субъектам персональных данных в случае в случае нарушения требований по обработке и обеспечению безопасности персональных данных (пункт 2.9.2 настоящего Положения);
- издает и утверждает приказом Руководителя документ, определяющий соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных;
- издает и утверждает приказом Руководителя перечень информационных систем персональных данных (пункт 2.18 настоящего Положения);
- издает и утверждает приказом Руководителя правила обработки персональных данных, определяющие:
 - цели обработки персональных данных содержание обрабатываемых персональных данных (пункты 2.3 настоящего Положения);
 - перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций (пункты 2.8 настоящего Положения);
 - перечень должностей сотрудников государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (пункт 2.19 настоящего Положения);
 - перечень должностей сотрудников государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (пункт 2.19 настоящего Положения);
 - типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного или муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (пункт 2.19 настоящего Положения);
 - порядок доступа сотрудников государственного или муниципального органа в помещения, в которых ведется обработка персональных данных (пункт 2.20 настоящего Положения);
 - принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные законодательством Российской Федерации в области персональных данных (пункт 3 настоящего Положения);
 - осуществляют ознакомление сотрудников государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных сотрудников (пункты 2.19 и 3.8 настоящего Положения);
 - уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных (пункт 2.16 настоящего Положения).

Указанные документы, являются определяющими политику в отношении обработки персональных данных в Организации и подлежат опубликованию на ее официальном сайте в течение 10 дней после их утверждения. К указанным документам обеспечивается неограниченный доступ.

2.13.1.7. Процедуры, направленные на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий

К процедурам, направленным на предотвращение и выявление нарушений законодательства в

отношении обработки персональных данных и устранение таких последствий относятся:

- реализация мер, направленных на обеспечение выполнения оператором своих обязанностей (пункт 2.13.2.3 настоящего Положения);
- выполнение предусмотренных законодательством в области персональных данных обязанностей, возложенных на Организацию;
- личная ответственность сотрудников Организации, осуществляющих обработку либо осуществление доступа к персональным данным;
- организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы;
- организация внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством в области персональных данных и локальными актами Организации;
- сокращение объема обрабатываемых данных;
- сокращение должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- стандартизация операций осуществляемых с персональными данными;
- порядок доступа сотрудников Организации в помещения, в которых ведется обработка персональных данных;
- проведение необходимых мероприятий по обеспечению безопасности персональных данных и носителей их содержащих;
- проведение периодических проверок условий обработки персональных данных;
- повышение осведомленности сотрудников, занимающих должности, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным путем их ознакомления с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами Организации по вопросам обработки персональных данных и (или) организация обучения указанных сотрудников;
- блокирование, внесение изменений и уничтожение персональных данных в предусмотренных действующим законодательством в области персональных данных случаях;
- оповещение субъектов персональных данных в предусмотренных действующим законодательством в области персональных данных случаях;
- разъяснение прав субъектам персональных данных в вопросах обработки и обеспечения безопасности их персональных данных;
- оказание содействия правоохранительным органам, в случаях нарушений законодательства в отношении обработки персональных;
- публикация на официальном сайте Организации документов, определяющих политику в отношении обработки персональных данных.

Указанный перечень процедур, направленных на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий является открытым и может дополняться мероприятиями в конкретных случаях.

2.14. Порядок взаимодействия с субъектами персональных данных и иными лицами.

Настоящее Положение при определении порядка взаимодействия Организации с субъектами персональных данных устанавливает:

- сроки выполнения действий по защите прав субъектов персональных данных;
- требования по уведомлениям/предоставлению информации субъектов персональных данных и в иных случаях;
- требования к лицам, ответственным за организацию обработки персональных данных;
- порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав;
- порядок реагирования на обращения субъектов персональных данных;
- порядок действий при обращениях субъектов персональных данных;
- требования к форме запроса на предоставления персональных данных и сведений об операторе субъектом персональных данных;
- порядок и основание отказа субъекту персональных данных в предоставлении сведений о его персональных данных;
- порядок, форма предоставления персональных данных и сведений об операторе и объем предоставляемой информации;
- действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных;
- порядок реализации права субъекта персональных данных на обжалование действий или бездействия Организации;
- порядок действий при достижении целей обработки персональных данных и отзыве согласия на

обработку персональных данных;

- порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных.

2.14.1. Установленные сроки выполнения действий по защите прав субъектов персональных данных

В Организации устанавливаются следующие сроки по защите прав субъектов персональных данных:

- в случае если **сведения**, а также **обрабатываемые персональные данные были предоставлены** для ознакомления субъекту персональных данных **по его запросу**, субъект персональных данных вправе обратиться повторно в Организацию или направить ей повторный запрос в целях получения таких сведений, и ознакомления с такими персональными данными **не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса**, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

- в случае **отказа в предоставлении информации** о наличии персональных данных о соответствующем субъекте персональных данных **или персональных данных** субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Организация **обязана дать в письменной форме мотивированный ответ**, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, **в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя**;

- **в срок, не превышающий семи рабочих дней со дня предоставления** субъектом персональных данных или его представителем **сведений**, подтверждающих, что **персональные данные являются неполными, неточными или неактуальными**, Организация обязана внести в них необходимые изменения;

- **в срок, не превышающий семи рабочих дней со дня представления** субъектом персональных данных или его представителем **сведений**, подтверждающих, что такие **персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки**, Организация обязана уничтожить такие персональные данные;

- **в случае выявления неправомерной обработки** персональных данных, осуществляемой Организацией или лицом, действующим по ее поручению, **в срок, не превышающий трех рабочих дней с даты этого выявления**, обязана прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по его поручению;

- **в случае если обеспечить правомерность обработки персональных данных невозможно**, **в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки** персональных данных, обязана уничтожить такие персональные данные или обеспечить их уничтожение;

- **в случае достижения цели обработки** персональных данных Организация обязана прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) **в срок, не превышающий тридцати дней с даты достижения цели обработки** персональных данных, **если иное не предусмотрено договором**, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Организацией и субъектом персональных данных, **либо если Организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами**;

- **в случае отзыва субъектом персональных данных согласия на обработку** его персональных данных Организация обязана прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и **в случае, если сохранение персональных данных более не требуется для целей обработки** персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) **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 персональных данных, иным соглашением между оператором и субъектом персональных данных, **либо, если Организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами**;

- **в случае отсутствия возможности уничтожения** персональных данных в течение указанных сроков, Организация осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и обеспечивает уничтожение персональных данных **в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами**;

- Организация обязана рассмотреть возражение субъекта персональных данных **о принятии на основании исключительно автоматизированной обработки** персональных данных решений, порождающих юридические последствия в отношении него или иным образом затрагивающих его права и законные интересы, **в**

течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;

- Организация обязана сообщить в установленном порядке, субъекту персональных данных 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 персональных данных или его представителя **либо в течение тридцати дней с даты получения запроса субъекта** персональных данных или его представителя;

- Организация обязана сообщить в уполномоченный орган по защите прав субъектов персональных данных **по запросу** этого органа необходимую информацию **в течение тридцати дней с даты получения такого запроса**;

- **в случае подтверждения факта неточности персональных данных** Организация на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязана уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) **в течение семи рабочих дней со дня представления таких сведений** и снять блокирование персональных данных.

Установленные сроки обязательны к исполнению всеми должностными лицами Организации.

- **в случае изменения сведений**, указанных в уведомлении об обработке персональных данных, а также **в случае прекращения обработки** персональных данных Организация обязана уведомить об этом уполномоченный орган по защите прав субъектов персональных данных **в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки** персональных данных.

2.14.2. Требования по уведомлениям (предоставлению информации, разъяснениям) субъектов персональных данных и в иных случаях

Организация обязана осуществлять уведомления и предоставлять информацию в следующих случаях:

- Организация обязана **разъяснить** субъекту персональных данных **порядок принятия решения на основании исключительно автоматизированной обработки** его персональных данных и **возможные юридические последствия** такого решения, **предоставить возможность заявить возражение** против такого решения, а также **разъяснить порядок защиты** субъектом персональных данных **своих прав и законных интересов**;

- Организация обязана рассмотреть **возражение субъекта персональных данных о принятии на основании исключительно автоматизированной обработки** персональных данных решений, порождающих юридические последствия в отношении него или иным образом затрагивающих его права и законные интересы, в течение тридцати дней со дня его получения и **уведомить субъекта персональных данных о результатах рассмотрения такого возражения**;

- **если предоставление персональных данных является обязательным в соответствии с федеральным законом**, Организация обязана **разъяснить** субъекту персональных данных **юридические последствия отказа предоставить его персональные данные**;

- Организация обязана **предоставить** безвозмездно субъекту персональных данных или его представителю **возможность ознакомления с персональными данными**, относящимися к этому субъекту персональных данных;

- Организация обязана **уведомить** субъекта персональных данных или его представителя **о внесенных изменениях и предпринятых мерах** в случаях когда персональные данные являются неполными, неточными или неактуальными и персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки и **принять разумные меры для уведомления третьих лиц**, которым персональные данные этого субъекта были переданы;

- **об устранении допущенных нарушений или об уничтожении** персональных данных **в случае выявления неправомерной обработки** персональных данных Организация **обязана уведомить субъекта персональных данных** или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос **уполномоченного органа по защите прав субъектов персональных данных** были направлены уполномоченным органом по защите прав субъектов персональных данных, также **указанный орган**;

- Организация **до начала обработки** персональных данных **обязана уведомить уполномоченный орган по защите прав субъектов персональных данных** о своем намерении осуществлять обработку персональных данных;

- **в случае изменения сведений**, а также **в случае прекращения обработки** персональных данных Организация обязана **уведомить об этом уполномоченный орган по защите прав субъектов персональных данных**;

- обязанность **предоставить доказательство получения согласия** субъекта персональных данных на обработку его персональных данных или **доказательство наличия иных законных оснований** возлагается на оператора;

- персональные данные **могут быть получены** Организацией **от лица, не являющегося субъектом**

персональных данных, **при условии предоставления им подтверждения наличия законных оснований** обработки, в том числе передачи таких персональных данных;

- Организацией **должны быть предоставлены** субъекту персональных данных запрашиваемые им сведения в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных;

- сведения, запрашиваемые субъектом персональных данных, **предоставляются** субъекту персональных данных или его представителю Организацией **при обращении либо при получении запроса** субъекта персональных данных или его представителя;

- обязанность **представления доказательств обоснованности** мотивированного **отказа** в выполнении повторного запроса субъекта персональных данных лежит на Организации;

- Организация обязана **разъяснить** субъекту персональных данных **порядок принятия решения на основании исключительно автоматизированной обработки** его персональных данных и **возможные юридические последствия** такого решения, **предоставить возможность заявить возражение** против такого решения, а также **разъяснить порядок защиты** субъектом персональных данных **своих прав и законных интересов**;

- **при сборе** персональных данных Организация обязана по просьбе субъекта персональных данных **предоставить** информацию, касающуюся обработки его персональных данных;

- если персональные данные получены не от субъекта персональных данных, Организация, до начала обработки таких персональных данных обязана предоставить субъекту персональных данных информацию, касающуюся обработки его персональных данных;

- Организация **по запросу** уполномоченного органа по защите прав субъектов персональных данных обязана **представить** документы и локальные акты, и (или) иным образом **подтвердить принятие мер**, направленных на обеспечение выполнения оператором обязанностей, предусмотренных действующим законодательством в области персональных данных;

- Организация обязана **сообщить** субъекту персональных данных 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 персональных данных или его представителя;

- Организация обязана **предоставить** безвозмездно субъекту персональных данных или его представителю **возможность ознакомления** с персональными данными, относящимися к этому субъекту персональных данных;

- Организация обязана **уведомить** субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах **в случае выявления того, что персональные данные являются неполными, неточными или неактуальными или являются незаконно полученными или не являются необходимыми для заявленной цели обработки и принять разумные меры для уведомления третьих лиц**, которым персональные данные этого субъекта были переданы;

- Организация обязана **сообщить** в уполномоченный орган по защите прав субъектов персональных данных **по запросу этого органа** необходимую информацию;

- Организация обязана **предоставлять** лицу, ответственному за организацию обработки персональных данных в Организации сведения, предусмотренные действующим законодательством в области персональных данных.

Организация освобождается от обязанности предоставить субъекту персональных данных сведения об обрабатываемых персональных данных, относящихся к субъекту персональных данных, в случаях, если:

- субъект персональных данных уведомлен об осуществлении Организацией обработки его персональных данных;

- персональные данные получены Организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

- Организация осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

- предоставление субъекту персональных данных нарушает права и законные интересы третьих лиц.

Уведомление в указанных случаях готовится лицом, ответственным за организацию обработки персональных данных в Организации. Подготовленное уведомление утверждается Руководителем. Отправка уведомления осуществляется лицом, ответственным за организацию обработки персональных данных в Организации в установленные пунктом 2.14.1 настоящего Положения сроки.

Требования к уведомлению уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных и об изменении поданных сведений устанавливаются пунктом 2.16 настоящего Положения.

2.14.3. Лица, ответственные за организацию обработки персональных данных

В Организации лицом, ответственным за организацию обработки персональных данных **назначается начальник управления информатизации, информации, делопроизводства и административно-хозяйственной работы аппарата главы администрации Алексеевского района**. Лицо, ответственное за организацию обработки персональных данных в Организации, получает указания непосредственно от Руководителя и подотчетно ему.

Организация предоставляет лицу, ответственному за организацию обработки персональных данных сведения об обработке персональных данных в соответствии с требованиями действующего законодательства в области персональных данных.

Организация разрабатывает должностную инструкцию ответственного за организацию обработки персональных данных.

Основными обязанностями лица, ответственного за организацию обработки персональных данных в Организации являются:

- осуществление внутреннего контроля за соблюдением Организацией и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения сотрудников Организации положений законодательства Российской Федерации о персональных данных, приказов по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

2.14.4. Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав

Сотрудники Организации обязаны разъяснять субъектам персональных данных особенности обработки персональных данных и порядок защиты их прав в следующих случаях:

- при принятии решения на основании исключительно автоматизированной обработки его персональных данных – разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных, возможные юридические последствия такого решения, а также порядок защиты субъектом персональных данных своих прав и законных интересов;
- если предоставление персональных данных является обязательным в соответствии с федеральным законом – разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

Разъяснение субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав осуществляется сотрудниками Организации, осуществляющими непосредственные операции по обработке персональных данных или лицом, ответственным за организацию обработки персональных данных. Разъяснения осуществляются на основании настоящего Положения, правил обработки персональных данных в конкретных информационных системах персональных данных в Организации и действующего законодательства Российской Федерации в области персональных данных.

Для разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав используются официальный сайт Организации, стенды, раздаточный материал.

2.14.5. Порядок реагирования на обращения субъектов персональных данных

Все обращения субъектов персональных данных принимаются в письменном виде и подлежат учету, наряду с остальными входящими документами.

С целью соблюдения сроков по реагированию на обращения субъектов персональных данных они должны незамедлительно передаваться лицу, ответственному за организацию обработки персональных данных.

Ответы на обращения, не отвечающие требованиям, предъявляемым к ним действующим законодательством в области персональных данных, не производятся.

Передача ответов субъекту персональных данных осуществляется требуемым им способом, или, если такой способ не указан, посредством отправки заказного письма с уведомлением.

Передача ответов на обращения субъектов персональных данных в Организации осуществляется в установленном порядке для исходящей корреспонденции с соблюдением указанных в пункте 2.14.1 настоящего Положения сроков.

2.14.6. Порядок действий при обращениях субъектов персональных данных

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, при личном обращении в Организацию, либо путем направления запроса, в том числе в форме электронного документа, подписанного электронной подписью в соответствии с законодательством

2.14.6.1. Требования к форме запроса на предоставления персональных данных и сведений об операторе субъектом персональных данных

Письменный запрос субъекта персональных данных на получение информации, касающейся обработки его персональных данных Организацией должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных;
- подпись субъекта персональных данных или его представителя.

Письменные запросы, не отвечающие указанным требованиям, обработке не подлежат.

При личном обращении в Организацию субъект персональных данных обязан предъявить документ, удостоверяющий его личность, а его представитель – документ, удостоверяющий личность представителя и документы, подтверждающие полномочия этого представителя, и сообщить сведения, подтверждающие участие субъекта персональных данных в отношениях с Организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных.

Данные предоставляемые субъектом персональных данных при личном обращении в Организацию фиксируется в Журнале учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана.

2.14.6.2. Порядок и основание отказа субъекту персональных данных в предоставлении сведений о его персональных данных

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в следующих случаях если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

В случае отказа в предоставлении субъекту персональных данных при обращении информации, касающейся обработки его персональных данных Организацией, либо при получении запроса субъекта персональных данных о такой информации, лицо, ответственное за организацию обработки персональных данных, составляет в письменной форме мотивированный ответ, содержащий ссылку на пункты или статьи федерального закона, являющегося основанием для такого отказа.

2.14.6.3. Порядок, форма предоставления персональных данных и сведений об операторе и объем предоставляемой информации

Предоставление доступа к своим персональным данным в случае непосредственного обращения субъекта персональных данных осуществляется только по адресу: Воронежская область, с. Новая Усмань, ул Советская, д.1, администрация Новоусманского муниципального района Воронежской области. Доступ субъекта персональных данных в этом случае осуществляется в порядке, установленном в пункте 2.14.6.1 настоящего Положения.

Субъект персональных данных имеет право на получение при обращении или при подаче запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Организацией;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения Организации, сведения о лицах (в том числе о сотрудниках Организации в объеме, предусмотренном пунктом 2.12 настоящего Положения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Организацией или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством в области персональных данных;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством в области персональных данных или другими федеральными законами.

Ответ на обращения и запросы субъектов персональных данных готовится лицом, ответственным за организацию обработки персональных данных, по существу такого обращения в двух экземплярах. Запрашиваемые сведения предоставляются в соответствии с настоящим Положением, Правилами обработки персональных данных в Организации и действующего законодательства Российской Федерации в области персональных данных.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Форму предоставления данных определяет лицо, ответственное за организацию обработки персональных данных, если она не оговорена в таком обращении или запросе. Форма ответа на обращение или запрос субъекта персональных данных не должна противоречить установленным в Организации требованиям по защите информации и обеспечению безопасности персональных данных.

Хранение информации об обращении или запрос субъекта персональных данных, а так же второй экземпляр ответа на такое обращение или запрос, хранятся установленным в Организации порядке.

2.14.6.4. Действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Организация осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Организация осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Организация на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снимает блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой Организацией или лицом, действующим по поручению оператора, Организация прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Организации.

В случае если обеспечить правомерность обработки персональных данных невозможно, Организация уничтожает такие персональные данные или обеспечивает их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Организация уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

При совершении указанных действий должны соблюдаться сроки, установленные в пункте 2.14.1 настоящего Положения.

При обнаружении нарушений правил обработки или обеспечения безопасности персональных данных лицо, ответственное за организацию обработки персональных данных в Организации незамедлительно принимает меры по устранению таких нарушений и минимизации их последствий. При этом должен проводиться анализ таких нарушений и приниматься меры по их недопущению в дальнейшем.

В случае если произошло нарушение прав субъекта персональных данных и данное нарушение может повлиять на нарушение прав такого субъекта в дальнейшем, Организация организует оповещение этого субъекта о возможных последствиях выявленных нарушений и принятых по ним мер. Порядок

такого оповещения устанавливается в каждой конкретной ситуации лицом, ответственным за организацию обработки персональных данных.

2.14.6.5. Право на обжалование действий или бездействия оператора

Если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований законодательства в области персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

2.14.7. Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных

В случае достижения цели обработки персональных данных Организация обязана прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации).

При совершении указанных действий должны соблюдаться сроки, установленные в пункте 2.14.1 настоящего Положения.

2.14.8. Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Организация обязана прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации).

При совершении указанных действий должны соблюдаться сроки, установленные в пункте 2.14.1 настоящего Положения.

2.15. Согласие субъекта персональных данных на обработку его персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Организацией.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, при которых такое согласие не требуется, возлагается на Организацию.

В Организации обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование, адрес Организации или иного оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых в Организации способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- дата предоставления согласия;
- подпись субъекта персональных данных.

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

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

Персональные данные могут быть получены Организацией от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, что обработка персональных данных может осуществляться без получения согласия.

Согласие субъекта персональных данных оформляется в двух экземплярах, один из которых передается субъекту персональных данных, а второй – Организации.

При документальном оформлении действий (операций) с персональными данными необходимо обратить особое внимание на использование термина «распространение» персональных данных, так как это действия, направленные на раскрытие персональных данных **неопределенному кругу лиц**, что при обработке персональных данных чаще всего является запрещенным. **Указанный термин «распространение» необходимо указывать только при обработке общедоступных данных.**

2.16. Уведомление об обработке (о намерении осуществлять обработку) персональных данных

Организация уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

При этом должны соблюдаться установленные настоящим Положением (пункт 2.14.1) сроки подачи уведомлений.

Организация вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- обрабатываемых в соответствии с трудовым законодательством;
- полученных Организацией в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Организацией исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- относящихся к членам (участникам) общественного объединения и обрабатываемых соответствующими общественным объединением, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;
- сделанных субъектом персональных данных общедоступными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится Организация, или в иных аналогичных целях;
- обрабатываемых 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.

Уведомление готовится лицом, ответственным за организацию обработки персональных данных в Организации, подписывается Руководителем и направляется в виде документа на бумажном носителе или в форме электронного документа.

Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

- описание мер направленных на обеспечение выполнения обязанностей, предусмотренных законодательством в области персональных данных и по обеспечению безопасности персональных данных при их обработке;
- фамилия, имя, отчество физического лица, ответственного за организацию обработки персональных данных в Организации, и номер его контактного телефона, почтовый адрес и адрес электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных.

Письменная форма уведомления устанавливается уполномоченным органом по защите прав субъектов персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения в реестр операторов.

Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

На Организацию не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

В случае предоставления неполных или недостоверных сведений, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от Организации уточнения предоставленных сведений до их внесения в реестр операторов.

В случае изменения сведений, а также в случае прекращения обработки персональных данных Организация обязана уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в сроки, указанные в пункте 2.14.1 настоящего Положения.

В случае изменения сведений, содержащихся в уведомлении об обработке персональных данных, структурное подразделение Организации, являющееся инициатором таких изменений в обработке персональных данных, готовит изменения в уведомление и передает такие изменения лицу, ответственному за организацию обработки персональных данных. Дальнейшие действия по подготовке изменений в уведомление для передачи в уполномоченный орган по защите прав субъектов персональных данных осуществляются аналогично действиям при первоначальной подаче уведомления.

2.17. Информационные системы персональных данных

К информационным системам персональных данных относятся совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. В Организации устанавливаются:

- критерии определения информационных систем персональных данных;
- наименование информационной системы персональных данных;
- цели создания или эксплуатации информационной системы персональных данных;
- параметры, характеризующие информационную систему персональных данных.

2.17.1. Критерии определения информационных систем персональных данных

Все информационные системы Организации, в которых производится обработка персональных данных, являются информационными системами персональных данных. Информационная система персональных данных состоит из совокупности:

- базы данных, в состав которой входят персональные данные;
- информационных технологий, позволяющих осуществлять обработку, содержащихся в базе данных персональных данных;
- технических средств, позволяющих осуществлять обработку, содержащихся в базе данных персональных данных.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных с помощью средств вычислительной техники является автоматизированной обработкой персональных данных.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Частным случаем автоматизированной обработки персональных данных является исключительно автоматизированная обработка персональных данных, при осуществлении которой решения, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, принимаются на основании исключительно автоматизированной обработки его персональных данных.

Обязательным условием создания информационной системы персональных данных является наличие **обособленной** базы данных, содержащей персональные данные, при изоляции которой от других информационных систем персональных данных, возможна обработка содержащихся в ней персональных данных с помощью информационных технологий и технических средств, входящих в состав этой информационной системы персональных данных.

Допускается использование одних и тех же информационных технологий и технических средств, для обработки различных баз данных, содержащих персональные данные, при этом разделение на различные информационные системы персональных данных производится по критерию уникальности баз данных, содержащих персональные данные.

2.17.2. Наименование информационной системы персональных данных

С целью идентификации каждой информационной системе персональных данных В Организации присваивается наименование, которое должно отражать основное назначение данной информационной системы либо наименование программных средств обработки персональных данных в данной информационной системе персональных данных.

2.17.3. Цели создания или эксплуатации информационной системы персональных данных

Для каждой информационной системы персональных данных определяются цели ее создания и эксплуатации. При этом определяется предполагаемое назначение информационной системы персональных данных, в соответствии с оказываемыми услугами, реализуемыми информационной системой персональных данных внутренними задачами или с определенными требованиями, предъявляемыми действующим в Российской Федерации законодательством.

2.17.4. Параметры, характеризующие информационную систему персональных данных

Для каждой информационной системы персональных данных Организации определяются следующие параметры, характеризующие такую информационную систему персональных данных:

- наименование информационной системы персональных данных;
- цели создания или эксплуатации информационной системы персональных данных;
- цель обработки персональных данных в информационной системе персональных данных;
- перечень персональных данных о субъекте персональных данных, обрабатываемых в информационной системе персональных данных;
- правовое основание обработки персональных данных в информационной системе персональных данных;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- действия (операции) с персональными данными;
- источники получения персональных данных;
- способы передачи персональных данных и их получатели;
- определение сроков обработки, в том числе хранения персональных данных в информационной системе персональных данных;
- заданные характеристики безопасности обрабатываемых в информационной системе персональных данных;
- места обработки персональных данных;
- характеристики средств автоматизации обработки персональных данных.

2.18. Перечень информационных систем персональных данных

Перечень информационных систем персональных данных Организации готовится лицом, ответственным за организацию обработки персональных данных и утверждается Руководителем.

Перечень информационных систем персональных данных Организации хранится у лица, ответственного за организацию обработки персональных данных

В Перечне информационных систем персональных данных Организации должна содержаться следующая информация:

- наименование информационной системы персональных данных;
- перечень структурных подразделений, осуществляющих эксплуатацию информационной системы персональных данных;
- перечень сотрудников Организации, осуществляющих обработку персональных данных;
- перечень средств вычислительной техники, участвующей в обработке персональных данных;

- структурное подразделение, ответственное за эксплуатацию информационной системы персональных данных.

С Перечнем информационных систем персональных данных в Организации под роспись должны быть ознакомлены все руководители структурных подразделений.

2.19. Требования к сотрудникам, осуществляющим доступ к персональным данным или их обработку

Организация осуществляет ознакомление своих сотрудников, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), распоряжениями Организации по вопросам обработки персональных данных, включая настоящее Положение:

- при оформлении договора, в том числе трудового;
- после каждого перерыва в исполнении своих обязанностей на срок более 28 рабочих дней;
- при первоначальном допуске к обработке персональных данных в информационной системе персональных данных;
- при назначении на новую должность, связанную с обработкой персональных данных или доступом к ним;
- после внесения изменений в действующее законодательство Российской Федерации о персональных данных, локальные акты Организации по вопросам обработки персональных данных, включая настоящее Положение.

Сотрудники Организации, непосредственно осуществляющие обработку персональных данных или осуществляющие доступ к ним обязаны:

- неукоснительно следовать принципам обработки персональных данных (пункт 2.2 настоящего Положения);
- знать и строго соблюдать положения действующего законодательства Российской Федерации в области персональных данных;
- знать и строго соблюдать положения локальных актов Организации в области обработки и обеспечения безопасности персональных данных;
- знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдать конфиденциальность персональных данных, то есть не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- не допускать нарушений требований и правил обработки и обеспечения безопасности персональных данных;
- обо всех подозрениях и ставших известными случаях нарушений требований и правил обработки и обеспечения безопасности персональных данных сообщать лицу, ответственному за обработку персональных данных в Организации.

Сотрудники Организации несут личную ответственность за соблюдение указанных обязанностей в предусмотренном действующим законодательством Российской Федерации объеме.

2.20. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных

Доступ сотрудников Организации в помещения, в которых ведется обработка персональных данных, осуществляется по Спискам сотрудников Организации, допущенных в помещения, в которых ведется обработка персональных данных. Такие списки готовятся и уточняются лицом, ответственным за организацию обработки персональных данных и утверждаются Руководителем.

Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется сотрудниками, указанными в Списках сотрудников Организации, допущенных в помещения, в которых ведется обработка персональных данных. Пребывание таких посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии сотрудников, указанных в Списках сотрудников Организации, допущенных в помещения, в которых ведется обработка персональных данных.

3. Конфиденциальность персональных данных

Запрет раскрытия третьим лицам и распространения персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, Организацией и иными лицами, получившим доступ к персональным данным называется конфиденциальностью персональных данных.

3.1. Режим ограниченного доступа к персональным данным

С целью реализации требований действующего законодательства Российской Федерации в Белгородской области персональных данных по обеспечению конфиденциальности персональных данных в Организации вводится режим ограниченного доступа к персональным данным.

Создание режима ограниченного доступа к персональным данным включает в себя:

- создание и уточнение Перечня информационных систем персональных данных в Организации;
- создание и уточнение настоящего Положения в части касающейся обеспечения конфиденциальности персональных данных и обеспечения безопасности персональных данных;
- создание и уточнение Перечня помещений, предназначенных для обработки персональных данных;
- перечень должностей сотрудников Организации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- определение технических средств обработки персональных данных, путем разработки, оформления и уточнения Технического паспорта (или Технических паспортов) информационных систем персональных данных Организации;
- разработки, оформления и уточнения Перечня информационных ресурсов, содержащих персональные данные (мест расположения баз данных или иных документов и массивов, содержащих персональные данные);
- создание комиссии по классификации и обследованию помещений, предназначенных для обработки персональных данных;
- создание классификации помещений, предназначенных для обработки персональных данных на предмет соответствия требованиям к инженерно-технической укрепленности по защите объектов от преступных посягательств;
- дополнение в гражданско-правовые договоры с контрагентами по вопросам обязательства по обеспечению охраны конфиденциальности информации и ответственности за обеспечение охраны ее конфиденциальности;
- внесение изменений в должностные обязанности (дополнения в трудовой договор сотрудников), предусматривающие регулирование отношений по использованию информации, ограниченного доступа;
- получение расписок об ознакомлении сотрудниками Организации, доступ которых к информации ограниченного доступа, обладателями которой являются Организация, ее контрагенты и клиенты, необходимо для выполнения ими своих трудовых обязанностей, с перечнем информации ограниченного доступа, установленным режимом ограничения доступа к информации и мерами ответственности за его нарушение;
- передачу (возврат) сотрудниками Организации при прекращении или расторжении трудового договора, имеющих в пользовании такого сотрудника материальных носителей информации, содержащих персональные данные;
- проведение начальных и периодических занятий и иных мероприятий по повышению уровня знаний сотрудников Организации, допущенных к обработке персональных данных по вопросам обработки и обеспечения безопасности персональных данных;
- создание и ведение Журнала регистрации машинных носителей информации;
- создание и ведение Журнала учета сейфов, металлических шкафов, спецхранов и ключей от них;
- создание и ведение списков лиц, имеющих доступ в помещения, в которых обрабатываются персональные данные;
- создание и ведение Журнала (-ов) приема (сдачи) под охрану помещений, в которых осуществляется обработка персональных данных;
- документирование и реализация разрешительной системы доступа (матриц доступа) к информационным (программным) ресурсам в автоматизированных системах информационных систем персональных данных Организации;
- разработка инструкций о действиях сотрудников Организации в отношении носителей персональных данных при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров, нарушениях правопорядка и др.);
- разработка инструкций для сотрудников Организации по вопросам обеспечения безопасности персональных данных.

Организация и контроль за выполнением указанных мероприятий возлагается на лицо, ответственное за организацию обработки персональных данных в Организации. Разрабатываемые документы подлежат утверждению Руководителем.

3.2. Порядок учета и маркирования материальных носителей информации, образующихся в процессе обработки персональных данных

С целью реализации режима ограниченного доступа к персональным данным В Организации и недопущению бесконтрольного использования машинных носителей, содержащих персональные данные, вводится их поэкземплярный учет.

Организация и контроль за выполнением учета машинных носителей, содержащих персональные данные, возлагается на лицо, ответственное за организацию обработки персональных данных в Организации.

Учет машинных носителей, содержащих персональные данные, осуществляется по Журналу учета машинных носителей информации.

4. Обеспечение безопасности персональных данных при их обработке

В соответствии с требованиями действующего законодательства в области персональных данных при обработке персональных данных Организация обязана принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах Организации являются неотъемлемой частью работ по созданию информационных систем.

4.1. Принципы обеспечения безопасности персональных данных при их обработке

Обеспечение безопасности персональных данных в Организации должно осуществляться на основе следующих принципов:

- соблюдение конфиденциальности персональных данных и иных характеристик их безопасности;
- реализация права на доступ к персональным данным лиц, доступ которых разрешается в рамках действующего законодательства Российской Федерации и распоряжениями Организации;
- обеспечение защиты информации, содержащей персональные данные, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

Категорически запрещается нарушать указанные принципы по обеспечению безопасности персональных данных.

4.2. Требования по уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, информационные системы персональных данных классифицируются в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
 - присвоение информационной системе соответствующего класса и его документальное оформление.
- При проведении классификации информационной системы учитываются следующие исходные данные:
- категория обрабатываемых в информационной системе персональных данных;
 - объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
 - заданные характеристики безопасности персональных данных, обрабатываемых в информационной системе;
 - структура информационной системы;
 - наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
 - режим обработки персональных данных;
 - режим разграничения прав доступа пользователей информационной системы;
 - местонахождение технических средств информационной системы.

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

Результаты классификации информационных систем оформляются соответствующим Актом классификации.

4.3. Состав мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных должны носить комплексный характер и включать в себя правовые, организационные и технические меры, описанные в настоящем Положении.

Порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются настоящим Положением.

4.3.1. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

Ответственным за организацию и контроль за обеспечение безопасности персональных данных В Организации при обработке персональных данных, осуществляемой без использования средств автоматизации, является лицо, ответственное за организацию обработки персональных данных.

4.3.2. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации

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

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

К методам и способам защиты информации в информационных системах персональных данных относятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);
- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных

данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

Методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами, основными методами и способами защиты информации от несанкционированного доступа являются:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- использование средств антивирусной защиты;
- централизованное управление системой защиты персональных данных информационной системы.

Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах I класса могут применяться следующие методы и способы защиты информации:

- использование технических средств в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

В информационных системах 2 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

При применении в информационных системах функции голосового ввода персональных данных в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для информационной системы 1 класса реализуются методы и способы защиты акустической (речевой) информации.

Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационную систему или воспроизведении информации акустическими средствами.

Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки персональных данных в информационной системе.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств, в том числе средств криптографической защиты информации.

4.4. Система защиты персональных данных

Безопасность персональных данных при их обработке в информационных системах Организации обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Разработка системы защиты персональных данных, частная модель угроз, осуществляется специализированной организацией на основании специального разрешения (лицензии) на осуществление данного вида деятельности.

4.4.1. Частная модель угроз.

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

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

Под угрозами безопасности персональных данных при их обработке в информационной системе персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Модель угроз решает следующие задачи:

- анализ защищенности информационной системы персональных данных от угроз безопасности персональных данных в ходе выполнения работ по обеспечению безопасности персональных данных;
- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационной системы персональных данных;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационной системы персональных данных, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

Модель угроз безопасности персональных данных при их обработке в информационных системах

персональных данных Организации должна содержать систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных, обусловленных преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационной системе персональных данных, связанным:

- с перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в информационной системе персональных данных с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы информационной системы персональных данных и обрабатываемых в них персональных данных с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования персональных данных.

Состав и содержание угроз безопасности персональным данным определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным.

Совокупность таких условий и факторов формируется с учетом характеристик информационной системы персональных данных, свойств среды распространения информативных сигналов, содержащих защищаемую информацию, и возможностей и источников угроз.

При обеспечении безопасности персональных данных с использованием криптографических средств защиты информации производится нейтрализация атак, готовящимися и проводимыми нарушителями, причем возможности проведения атак обусловлены их возможностями. С учетом этого все возможные атаки определяются моделью нарушителя.

4.4.2. Средства защиты информации

Средства защиты информации, применяемые в информационных системах персональных данных, в установленном порядке проходят процедуру оценки соответствия.

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

Эксплуатация средств защиты информации должна осуществляться строго в соответствии с эксплуатационной документацией на такие средства. Сотрудники Организации, эксплуатирующие средства защиты информации, должны быть ознакомлены с такой документацией под роспись.

4.5. Требования к помещениям, в которых производится обработка персональных данных

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

В Организации специальное оборудование помещений, в которых ведется работа с персональными данными, осуществляется в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств».

Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, соответствуют требованиям пожарной безопасности, установленными действующим законодательством Российской Федерации.

4.6. Порядок оценки соответствия требованиям по безопасности персональных данных

Порядок оценки соответствия информационных систем персональных данных требованиям безопасности информации осуществляется в порядке, определяемом действующим законодательством Российской Федерации и Программой такой оценки. Программу проведения оценочных испытаний разрабатывает организация, проводящая такую оценку. Программа согласовывается с Организацией.

Программа оценки соответствия информационных систем персональных данных требованиям безопасности информации содержит:

- перечень работ и их продолжительность;
- методики испытаний (или используются типовые методики);
- количественный и профессиональный состав оценочной комиссии;
- необходимость использования контрольной аппаратуры и тестовых средств.

Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей,

соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

По результатам оценки соответствия информационных систем персональным данным требованиям безопасности информации оформляются протоколы и заключение о соответствии таким требованиям. На основании заключения, в случае получения положительного решения о соответствии информационной системы персональным данным предъявляемым требованиям по обеспечению безопасности персональных данных, оформляется документ, подтверждающий выполнение требований по безопасности информации.

5. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных

Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных в Организации состоит из следующих направлений:

- внешний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных;
- внутренний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных.

Внутренний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных в Организации состоит из:

- контроля и надзора за исполнением требований по обработке и обеспечению безопасности персональных данных;
- оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

5.1. Порядок внешнего контроля над соблюдением требований по обработке и обеспечению безопасности данных

Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи, федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации в области защиты прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, подзаконных нормативных актов Правительства Российской Федерации, ведомственных нормативных актов и административных регламентов.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

Уполномоченный орган по защите прав субъектов персональных данных имеет право:

- запрашивать у Организации информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных Организации, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от Организации уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства в области персональных данных;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;
- направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, необходимые сведения;
- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

- привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

5.2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Организации организуется проведение периодических проверок условий обработки персональных данных. Проверки осуществляются ответственным за организацию обработки персональных данных либо комиссией, образуемой Руководителем не реже одного раза в год.

При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в Организации производится проверка:

- соблюдения принципов обработки персональных данных в Организации;
- соответствия приказов (распоряжений) в области персональных данных Организации действующему законодательству Российской Федерации;
- выполнения сотрудниками Организации требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных Организации;
- перечней персональных данных, используемых для решения задач и функций структурными подразделениями Организации и необходимости обработки персональных данных в информационных системах персональных данных;
- актуальности содержащихся в Правилах обработки персональных данных в каждой информационной системе персональных данных Организации информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- правильность осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных Организации;
- актуальность перечня должностей сотрудников Организации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- актуальность перечня должностей сотрудников Организации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Организации;
- соблюдение обязанностей Организацией, предусмотренных действующим законодательством в области персональных данных;
- порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Организации, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;
- наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Организации;
- актуальность сведений, содержащихся в уведомлении Организации об обработке персональных данных;
- актуальность перечня информационных систем персональных данных в Организации;
- наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных Организации;
- знания и соблюдение сотрудниками Организации положений действующего законодательства Российской Федерации в области персональных данных;
- знания и соблюдение сотрудниками Организации положений локальных актов Организации в

области обработки и обеспечения безопасности персональных данных;

- знания и соблюдение сотрудниками Организации инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдение сотрудниками Организации конфиденциальности персональных данных;
- актуальность приказов (распоряжений) Организации в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;
- соблюдение сотрудниками Организации требований по обеспечению безопасности персональных данных;
- наличие приказов (распоряжений) Организации, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных;
- иных вопросов.

Ответственный за организацию обработки персональных данных в Организации либо председатель комиссии докладывает Руководителю о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений.

5.3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных

Во время осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Организации производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в Организации.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, для каждой информационной системы персональных данных Организации производится экспертное сравнение заявленной Организацией в своих приказах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (пункт 2.9.2 настоящего Положения) и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и изложенных в настоящем Положении.

По итогам сравнений принимается решение о достаточности применяемых Организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и возможности или необходимости принятия дополнительных мер или изменения установленного в Организации порядка обработки и обеспечения безопасности персональных данных.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в Организации оформляется в виде отдельного документа, подписывается лицом, ответственным за организацию обработки персональных данных либо председателем комиссии, и утверждается Руководителем.

По результатам принятых решений, лицом, ответственным за организацию обработки персональных данных в Организации и организуется работа по их реализации.

6. Ответственность за нарушение требований в области персональных данных

Лица, виновные в нарушении требований действующего законодательства в области персональных данных, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

7. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае появления обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые Организация не могла предвидеть и предотвратить разумными мерами, должностные лица Организации обязаны принять все возможные меры по недопущению нарушения прав субъектов персональных данных.

К обстоятельствам непреодолимой силы относятся события, на которые Организация не могла оказывать влияние и за возникновение которых он не несет ответственности: землетрясение, наводнение, пожар,

забастовки, насильственные или военные действия любого характера, решения органов государственной власти препятствующие исполнению требований законодательства в области персональных данных.

Надлежащим доказательством наличия указанных выше обстоятельств будут служить официальные документы Организации и органов государственной власти Российской Федерации.

Организация в случае возникновения указанных выше обстоятельств и нарушении прав субъектов персональных данных, связанных с такими обстоятельствами, извещает субъектов персональных данных всеми доступными способами.

8. Мероприятия по обработке персональных данных при проведении процедур ликвидации или реорганизации

При ликвидации Организации все носители персональных данных подлежат уничтожению установленными настоящим Положением способами, за исключением носителей, подлежащих в соответствии с действующим законодательством Российской Федерации передаче в организацию-учредитель Организации.

При реорганизации Организации в форме слияния, присоединения и преобразования решение о необходимости уничтожения персональных данных или передачи их образуемому учреждению принимается в соответствии с действующим законодательством Российской Федерации.

9. Ознакомление субъектов персональных данных с документами, определяющими политику в отношении обработки персональных данных

Настоящее Положение, а также иные документы, определяющие политику в отношении обработки персональных данных, публикуются на официальном сайте Организации по адресу: <http://www.nusman.ru/> в течение 10 дней после их утверждения.

Ответственными за публикацию настоящего Положения, а также иных документов, определяющих политику в отношении обработки персональных данных в Организации, а так же изменений к ним, являются:

- сотрудник, осуществляющий взаимодействие со СМИ (связь с общественностью);
- сотрудник, осуществляющий техническое сопровождение web-представительства (размещение информации);
- ответственный за организацию обработки персональных данных в Организации.

Лицом, ответственным за организацию обработки персональных данных в Организации обеспечивается неограниченный доступ к настоящему Положению, а также иным документам, определяющим политику в отношении обработки персональных данных в Организации любых заинтересованных лиц при личном приеме либо по запросу, совершаемому в соответствии с действующим законодательством Российской Федерации.

10. Руководящие документы, используемые в настоящем Положении

В настоящем Положении использованы следующие руководящие документы:

- Федеральный закон РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных» в редакции от 25.07.2011 г. № 261;
- Федеральный закон РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ № 781 от 17.11.2007 г. «Об утверждении Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 г. № 230-ФЗ;
- Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 г.);
- Постановление Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Приказ ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных».