



**АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
СЕННОЙ ОКРУГ
САНКТ-ПЕТЕРБУРГ**

=====

190031, Санкт-Петербург, наб. р. Фонтанки, д.89 тел./факс 310-16-96 e-mail: msmoso@mail.wplus.net

**Постановление № 88
10 мая 2017 года**

Об утверждении нормативно-правовых актов в сфере защиты персональных данных

В целях соблюдения требований действующего законодательства в сфере защиты персональных данных,

Администрация Внутригородского муниципального образования Санкт-Петербурга муниципального округа Сенной округ

ПОСТАНОВИЛА:

1. Утвердить ПОЛИТИКУ в отношении обработки персональных данных в Администрации МО Сенной округ согласно приложению № 1.
2. Утвердить ПОРЯДОК хранения, использования и передачи персональных данных сотрудников Администрации МО Сенной округ согласно приложению № 2.
3. Утвердить ПОЛОЖЕНИЕ по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ согласно приложению № 3.
4. Обнародовать настоящее решение путем размещения на стендах.
5. Постановление вступает в силу с момента его обнародования.
6. Контроль за исполнением Постановления возложить на Главу Администрации К.И. Кузьмичеву.

Глава Администрации

К.И. Кузьмичева

ПОЛИТИКА

в отношении обработки персональных данных в Администрации МО Сенной округ

ОСНОВНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика в отношении обработки персональных данных в Администрации МО Сенной округ (далее – Политика) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 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».

Политика вступает в силу с момента ее утверждения руководителем Администрации МО Сенной округ (далее – Администрация, Оператор).

Политика подлежит пересмотру в ходе периодического анализа со стороны руководства Администрации, а также в случаях изменения законодательства Российской Федерации в области персональных данных.

Политика подлежит опубликованию на официальном сайте Администрации в течение 10 дней после её утверждения.

ЦЕЛИ

Целью Политики является обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных Администрацией.

ОСНОВНЫЕ ПОНЯТИЯ

Для целей Политики используются следующие 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;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

ОБЛАСТЬ ДЕЙСТВИЯ

Положения Политики распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой Администрацией:

– с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

– без использования средств автоматизации.

Политика применяется ко всем сотрудникам Администрации.

ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных осуществляется Администрацией в следующих целях:

- выполнение требований трудового законодательства Российской Федерации и законодательства о муниципальной службе Российской Федерации в части ведения бухгалтерского учета, исполнение условий договоров гражданско-правового характера;
- выполнение требований трудового законодательства Российской Федерации и законодательства о муниципальной службе Российской Федерации и гор. Санкт-Петербурга в части ведения кадрового учета, заключение служебных контрактов, трудовых и иных договоров, ведение личных дел (карточек), ведение воинского учета;
- рассмотрение обращений граждан;
- осуществление и выполнение возложенных законодательством гор. Санкт-Петербурга функций, полномочий и обязанностей по опеке и попечительству;
- осуществление и выполнение возложенных законодательством гор. Санкт-Петербурга функций, полномочий и обязанностей по составлению протоколов об административных правонарушениях.

КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

6.1. В соответствии с целями обработки персональных данных, указанными в п.5 настоящей Политики, Администрацией осуществляется обработка следующих категорий субъектов персональных данных:

- муниципальные служащие;
- работники, замещающие должности, не являющиеся должностями муниципальной службы, и рабочие;
- граждане, персональные данные которых необходимы для выполнения возложенных законодательством гор. Санкт-Петербург функций, полномочий и обязанностей по опеке и попечительству;
- граждане, состоящие с Администрацией в гражданско-правовых отношениях;
- близкие родственники муниципальных служащих, персональные данные которых необходимы в целях выполнения требований законодательства о муниципальной службе Российской Федерации;
- близкие родственники работников, замещающих должности, не являющиеся должностями муниципальной службы, и рабочих, персональные данные которых необходимы в целях выполнения требований трудового законодательства Российской Федерации;
- граждане, персональные данные которых необходимы для рассмотрения обращений граждан.

6.2. Перечень обрабатываемых персональных данных утвержден нормативным актом Администрации.

АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Принципы обработки персональных данных

Обработка персональных данных осуществляется Администрацией в соответствии со следующими принципами:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается 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 соответствуют заявленным целям обработки; обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных; Администрация принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных осуществляется 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.

Условия обработки персональных данных

Условия обработки персональных данных, отличные от получения согласия субъекта персональных данных на обработку его персональных данных являются альтернативными.

7.1.1. Условия обработки специальных категорий персональных данных

Обработка специальных категорий персональных данных осуществляется Администрацией с соблюдением следующих условий:

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

7.1.2. Условия обработки биометрических персональных данных

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Администрацией для установления личности субъекта персональных данных Администрацией не обрабатываются.

7.1.3. Условия обработки иных категорий персональных данных

Обработка иных категорий персональных данных осуществляется Администрацией с соблюдением следующих условий:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию МО Сенной округ функций, полномочий и обязанностей;
- 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 осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

7.1.4. Условия обработки общедоступных персональных данных

Обработка общедоступных персональных данных Администрацией не производится.

7.1.5. Поручение обработки персональных данных

7.1.5.1. Администрация вправе 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 (далее – поручение).

7.1.5.2. Администрация поручает обработку следующих персональных данных:

– ФИО; должность; структурное подразделение; контактные телефоны: Общество с ограниченной ответственностью «Научно – производственный центр «Кейсистемс – Безопасность»;

– ФИО; дата рождения; место рождения; адрес регистрации; адрес проживания; контактные телефоны; данные документа, удостоверяющего личность; наименование органа, выдавшего документ, удостоверяющий личность; дата выдачи документа, удостоверяющего личность; должность; место работы; гражданство; банковские реквизиты; номер счета; сумма: Публичное акционерное общество «Сбербанк России».

7.1.5.3. Лицо, осуществляющее обработку персональных данных по поручению Администрации, соблюдает принципы и правила обработки персональных данных, предусмотренные настоящей Политикой. В поручении Администрации определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указаны требования к защите обрабатываемых персональных данных.

7.1.5.4. При поручении обработки персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Администрация. Лицо, осуществляющее обработку персональных данных по поручению Администрации, несет ответственность перед Администрацией.

Конфиденциальность персональных данных

7.2.1. Сотрудники Администрации, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Общедоступные источники персональных данных

7.3.1. Администрация не создает общедоступные источники персональных данных.

Согласие субъекта персональных данных на обработку его персональных данных

7.4.1. При необходимости обеспечения условий обработки персональных данных субъекта может предоставляться согласие субъекта персональных данных на обработку его персональных данных.

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

7.4.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Администрация вправе продолжить обработку персональных данных без согласия субъекта персональных данных при выполнении альтернативных условий обработки персональных данных.

7.4.4. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство выполнения альтернативных условий обработки персональных данных возлагается на Администрацию.

7.4.5. В случаях, предусмотренных федеральным законом, 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:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) 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);

3) наименование или фамилию, имя, отчество и адрес Оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

7.4.6. 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.

7.4.7. В случае недееспособности субъекта персональных данных согласие на обработку его

персональных данных дает законный представитель субъекта персональных данных.

7.4.8. 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.

7.4.9. Персональные данные могут быть получены Администрацией от лица, не являющегося субъектом персональных данных, при условии предоставления Администрации подтверждения наличия альтернативных условий обработки информации.

Трансграничная передача персональных данных

7.5.1. Трансграничная передача персональных данных Администрацией не осуществляется.

Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

7.6.1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

7.6.2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

7.6.3. 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 государственных или муниципальных 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 государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

7.6.4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Права субъектов персональных данных

7.7.1. *Право субъекта персональных данных на доступ к его персональным данным*

7.7.1.1. Субъект персональных данных имеет право на получение информации (далее – запрашиваемая субъектом информация), касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Администрацией;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые Администрацией способы обработки персональных данных;
- 4) наименование и место нахождения Администрации, сведения о лицах (за исключением работников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7.7.1.2. Субъект персональных данных имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

– обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

– обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

– 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;

– обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

7.7.1.3. Субъект персональных данных вправе требовать от Администрации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.7.1.4. Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных Администрацией 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.

7.7.1.5. Запрашиваемая информация предоставляется субъекту персональных данных или его представителю Администрацией при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос 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 Администрацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Администрацией, подпись субъекта персональных данных или его представителя (далее – необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.7.1.6. В случае если запрашиваемая субъектом информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения запрашиваемой субъектом информации, и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее – нормированный срок запроса) 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.

7.7.1.7. Субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми персональными данными до истечения нормированного срока запроса, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать обоснование направления повторного запроса.

7.7.1.8. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Администрации.

7.7.2. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

7.7.2.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации Администрацией не осуществляется.

7.7.3. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

7.7.3.1. 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 Администрацией не осуществляется.

7.7.4. Право на обжалование действий или бездействия Оператора

7.7.4.1. Если субъект персональных данных считает, что Администрация осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Администрации в

уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.7.4.2. 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.

Обязанности Оператора

7.8.1. Обязанности Оператора при сборе персональных данных

7.8.1.1. При сборе персональных данных Администрация предоставляет субъекту персональных данных по его просьбе запрашиваемую субъектом информацию.

7.8.1.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Администрация разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

7.8.1.3. Если персональные данные получены не от субъекта персональных данных, Администрация до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию (далее – информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

- 1) наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
- 5) источник получения персональных данных.

7.8.1.4. Администрация не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных Администрацией;
- 2) персональные данные получены Администрацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- 4) Администрация осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- 5) предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

7.8.1.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, обрабатываемых в следующих информационных системах:

7.8.1.5.1. Информационная система персональных данных «Бухгалтерский учет» с использованием баз данных, находящихся на территории России.

7.8.1.5.2. Информационная система персональных данных «Кадровый учет» с использованием баз данных, находящихся на территории России.

7.8.1.5.3. Информационная система персональных данных «Обращения граждан» с

использованием баз данных, находящихся на территории России.

7.8.1.5.4. Информационная система персональных данных «Опека и попечительство» с использованием баз данных, находящихся на территории России.

7.8.1.6. Местонахождение центра(ов) обработки данных и сведения об организации, ответственной за хранение данных, определены внутренними документами Администрации.

7.8.2. Меры, направленные на обеспечение выполнения Оператором своих обязанностей

7.8.2.1. Администрация принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. Администрация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

- 1) назначение ответственного за организацию обработки персональных данных;
- 2) издание Политики, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, Политике, локальным актам Оператора;
- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- 6) ознакомление сотрудников Администрации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, Политикой, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

7.8.3. Меры по обеспечению безопасности персональных данных при их обработке

7.8.3.1. Администрация при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает 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.

7.8.3.2. Обеспечение безопасности персональных данных достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 5) учетом машинных носителей персональных данных;
- 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

7.8.3.3. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться 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.

7.8.4. Обязанности Оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

7.8.4.1. Администрация сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет 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.

7.8.4.2. В случае отказа в предоставлении информации о наличии персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Администрация дает в письменной форме мотивированный ответ 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.

7.8.4.3. Администрация предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. 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, Администрация вносит 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, Администрация уничтожает такие персональные данные. Администрация уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.8.4.4. Администрация сообщает в уполномоченный орган по защите прав субъектов

персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

7.8.5. Обязанности Оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

7.8.5.1. 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 Администрация 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 Администрации) 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 Администрация осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации) 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.

7.8.5.2. В случае подтверждения факта неточности персональных данных Администрация 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 Администрации) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

7.8.5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Администрацией или лицом, действующим по поручению Администрации, Администрация в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Администрации. В случае если обеспечить правомерность обработки персональных данных невозможно, Администрация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Администрация 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.

7.8.5.4. В случае достижения цели обработки персональных данных Администрация прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению

Администрации) 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 Администрацией и субъектом персональных данных либо если Администрация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

7.8.5.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Администрация прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации) 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 Администрацией и субъектом персональных данных либо если Администрация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

7.8.5.6. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Администрация блокирует такие персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7.8.6. Уведомление об обработке персональных данных

7.8.6.1. Администрация, за исключением случаев, предусмотренных Федеральным законом «О персональных данных», до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

7.8.6.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление содержит следующие сведения:

- 1) наименование (фамилия, имя, отчество), адрес Оператора;
- 2) цель обработки персональных данных;
- 3) категории персональных данных;
- 4) категории субъектов, персональные данные которых обрабатываются;
- 5) правовое основание обработки персональных данных;
- 6) перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;
- 7) описание мер, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- 8) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- 9) дата начала обработки персональных данных;
- 10) срок или условие прекращения обработки персональных данных;

11) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

12) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

13) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

7.8.6.3. В случае изменения указанных сведений, а также в случае прекращения обработки персональных данных Администрация уведомляет 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.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМАЯ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Общие положения

8.0.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

8.1.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

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

8.1.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Администрации или лица, осуществляющие такую обработку по договору с Администрацией), проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Администрации.

8.1.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), соблюдаются следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат 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;

б) типовая форма предусматривает 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;

в) типовая форма составляется 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;

г) типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8.1.5. 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, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

а) 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;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

8.1.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Указанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

8.1.7. 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.

Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

8.3.1. Обработка персональных данных, осуществляемая без использования средств

автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

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

8.3.3. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Администрацией.

СФЕРЫ ОТВЕТСТВЕННОСТИ

Лица, ответственные за организацию обработки персональных данных в организациях

9.0.1. Администрация назначает лицо, ответственное за организацию обработки персональных данных.

9.0.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся Оператором, и подотчетно ему.

9.0.3. Администрация предоставляет лицу, ответственному за организацию обработки персональных данных, необходимые сведения.

9.0.4. Лицо, ответственное за организацию обработки персональных данных, в частности, выполняет следующие функции:

1) осуществляет внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводит до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

Ответственность

9.1.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

9.1.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О 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.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

При достижении целей ожидаются следующие результаты:

- обеспечение защиты прав и свобод субъектов персональных данных при обработке его персональных данных Администрацией;
- повышение общего уровня информационной безопасности Администрации;
- минимизация юридических рисков Администрации.

СВЯЗНЫЕ ПОЛИТИКИ

Связные политики отсутствуют.

ПОРЯДОК
хранения, использования и передачи персональных данных сотрудников Администрации
МО Сенной округ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок хранения, использования и передачи персональных данных сотрудников Администрации МО Сенной округ (далее – Порядок) разработан в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.2. Цель разработки настоящего Порядка – определение порядка обработки (хранения, использования, передачи) персональных данных сотрудников Администрации МО Сенной округ (далее – Администрация, Оператор); обеспечение защиты прав и свобод сотрудников Администрации при обработке их персональных данных.

2. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
СОТРУДНИКОВ

2.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудника Администрации, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является сотрудник. 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. Хранение персональных данных сотрудников Администрации может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

2.2. Все отчуждаемые машинные носители персональных данных подлежат строгому учету. Форма Журнала учета отчуждаемых машинных носителей персональных данных утверждена нормативным актом Администрации.

2.3. Персональные данные сотрудников, содержащиеся на машинных носителях персональных данных, должны храниться на автоматизированных рабочих местах и серверах информационных систем персональных данных Администрации, установленных в пределах помещений, утвержденных Приказом об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных.

2.4. Персональные данные сотрудников, содержащиеся на материальных носителях персональных данных, должны храниться в пределах помещений, утвержденных Приказом об обеспечении безопасности материальных носителей персональных данных.

2.5. Хранение персональных данных сотрудников должно происходить в порядке, исключающем их утрату или их неправомерное использование.

2.6. Использование персональных данных сотрудников Администрации осуществляется Администрацией исключительно в целях выполнения требований трудового законодательства Российской Федерации.

2.7. Обработка персональных данных сотрудников Администрации осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом Администрации, при этом указанные в приказе сотрудники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.

2.8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

2.9. Передача персональных данных сотрудников между структурными подразделениями Администрации осуществляется только между сотрудниками, включенными в перечень лиц, имеющих доступ к персональным данным.

2.10. Обработка персональных данных сотрудников должна осуществляться только в пределах помещений Администрации и с использованием средств вычислительной техники Администрации.

2.11. Администрация вправе поручить обработку персональных данных сотрудников другим юридическим или физическим лицам на основании договора (далее – поручение Администрации) с согласия сотрудника, если иное не предусмотрено Федеральным законом «О персональных данных». Лицо, осуществляющее обработку персональных данных по поручению Администрации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

2.12. Сотрудники Администрации и иные лица, получающие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия сотрудников, если иное не предусмотрено федеральным законодательством в сфере защиты персональных данных.

3. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. При передаче персональных данных сотрудника Оператор должен соблюдать следующие требования:

– не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

– предупреждать лица, получающие персональные данные сотрудников, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;

– не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия;

– передавать персональные данные сотрудника представителям сотрудников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функций;

– не отвечать на вопросы, связанные с передачей персональных данных сотрудника по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими сотрудниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.

3.2. В целях обеспечения контроля правомерности использования переданных по запросам персональных данных лицами, их получившими, сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма соответствующего Журнала утверждена нормативным актом Администрации.

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 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», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) Администрации МО Сенной округ (далее – Администрация, Оператор) на протяжении всего жизненного цикла ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за

информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности персональных данных – 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.

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.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПДн).

3.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

3.4. Выбор средств защиты информации для СЗПДн осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение Федерального закона «О персональных данных».

3.5. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн при их обработке в ИСПДн.

3.6. СЗПДн создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на создание СЗПДн.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка необходимых средств защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

3.7. Этап 1. Проведение предпроектного обследования и разработка технического задания на создание СЗПДн.

3.7.1. Назначение ответственного за организацию обработки ПДн Администрацией.

3.7.2. Определение целей обработки ПДн Администрацией.

3.7.3. Определение перечня ИСПДн Администрации и состава ПДн, обрабатываемых в ИСПДн.

3.7.4. Определение перечня обрабатываемых Администрацией ПДн.

3.7.5. Определение сроков обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.

3.7.6. Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

3.7.7. Определение режимов обработки ПДн в ИСПДн в целом и в отдельных

компонентах.

3.7.8. Назначение ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн. Для каждой ИСПДн может быть назначен отдельный Ответственный.

3.7.9. Назначение ответственного пользователя криптосредств, обеспечивающего функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждение перечня лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей криптосредств).

3.7.10. Определение перечня помещений, в которых размещены ИСПДн и материальные носители ПДн.

3.7.11. Определение конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

3.7.12. Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.

3.7.13. Формирование технических паспортов ИСПДн.

3.7.14. Разработка организационно-распорядительных документов (далее – ОРД), регламентирующих процесс обработки и защиты ПДн:

- Политика в отношении обработки персональных данных;
- Инструкции (ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИСПДн, пользователя ИСПДн, ответственного пользователя криптосредств);

- Раздел должностных инструкций сотрудников Администрации в части обеспечения безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

3.7.15. Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн сотрудником Администрации.

3.7.16. Утверждение форм уведомлений субъектов ПДн и форм журналов, необходимых в целях обеспечения безопасности ПДн.

3.7.17. Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с «Требованиями к защите ПДн при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

3.7.18. Определение типа угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных». Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

3.7.19. Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

- уровень защищенности ПДн при их обработке в ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- состав и содержание работ по этапам разработки и внедрения СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации.

3.8. Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

3.8.1. Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и/или не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

3.8.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Администрации. Применение технических мер должно быть регламентировано нормативным актом Администрации.

3.8.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.8.4. На стадии проектирования и создания СЗПДн для ИСПДн Администрации проводятся следующие мероприятия:

- разработка технического проекта СЗПДн;
- приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;
- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;
- реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;
- подготовка эксплуатационной документации на используемые средства защиты информации;
- корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

3.9. Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.9.1. На стадии ввода в ИСПДн (СЗПДн) осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);

– контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

3.9.2. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

4. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных (ПРИЛОЖЕНИЕ № 1). Внутренние проверки режима обработки и защиты ПДн Администрацией проводятся в соответствии с Планом внутренних проверок режима обработки и защиты персональных данных (ПРИЛОЖЕНИЕ № 2). По результатам проведения внутренней проверки составляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Администрации МО Сенной округ (ПРИЛОЖЕНИЕ № 3).

4.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн Администрации требованиям безопасности ПДн.

4.3. При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

4.4. В соответствии с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн Администрации необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

5. РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

5.1. Модернизация СЗПДн для функционирующих ИСПДн Администрации должна осуществляться в случае:

- изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

- изменения состава угроз безопасности ПДн в ИСПДн;

- изменения уровня защищенности ПДн при их обработке в ИСПДн;

- прочих случаях, по решению оператора.

5.2. В целях определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год ответственным за организацию обработки ПДн должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем Администрации.

5.3. Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей ПДн;

- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;

- нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

ПРИЛОЖЕНИЕ № 1

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ

**План мероприятий по защите персональных данных
в Администрации МО Сенной округ**

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников Оператора к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
6.	Ведение журналов учета отчуждаемых электронных носителей персональных данных, средств защиты информации	Постоянно	
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Оператором устанавливаются сроки обработки ПДн, которые документально подтверждаются в нормативных документах Оператора. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных»
11.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
13.	Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
14.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона

ПРИЛОЖЕНИЕ № 2

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ

План внутренних проверок режима обработки и защиты персональных данных в Администрации МО Сенной округ

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Ежегодно	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	При необходимости	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Ежегодно	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПДн, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн: - Уведомления о факте обработки ПДн без использования средств автоматизации; - Обязательства о соблюдении конфиденциальности ПДн; - Формы ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами Администрации МО Сенной округ по вопросам обработки ПДн; - Типового обязательства о прекращении обработки ПДн в случае расторжения служебного контракта (трудового договора); - Разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн	При необходимости	
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	При необходимости	
6.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Ежегодно	

7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	При необходимости	
8.	Проверка соблюдения условий хранения материальных носителей ПДн	Ежегодно	
9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн	При необходимости	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Администрации МО Сенной округ в отношении обработки ПДн	Ежегодно	
11.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия	При необходимости	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн	При необходимости	
15.	Контроль учета машинных носителей ПДн	Ежегодно	
16.	Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ПДн в ИСПДн	Ежегодно	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн	Ежегодно	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИСПДн	При необходимости	
19.	Контроль корректности настроек средств защиты информации	Ежегодно	
20.	Контроль за обеспечением резервного копирования	Ежегодно	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн	При необходимости	

ПРИЛОЖЕНИЕ № 3

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ

Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Администрации МО Сенной округ

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации МО Сенной округ от «___» _____ 20__ г.

1.2 Проверка проводилась «___» _____ 20__ г. по адресу:

1.3 В ходе проверки были проведены следующие мероприятия:

- 1) _____
- 2) _____
- 3) _____
- 4) _____
- 5) _____

1.4 Результаты проведения проверки:

- 1) _____
- 2) _____
- 3) _____
- 4) _____
- 5) _____

1.5 Необходимые мероприятия.

На основании проведения внутренней проверки режима обработки и защиты ПДн рекомендуется осуществить следующие мероприятия:

- 1) _____
- 2) _____
- 3) _____
- 4) _____
- 5) _____

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защиты ПДн:

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)