

**АДМИНИСТРАЦИЯ СОСНОВСКОГО МУНИЦИПАЛЬНОГО  
РАЙОНА НИЖЕГОРОДСКОЙ ОБЛАСТИ  
ПОСТАНОВЛЕНИЕ**

18.09.2020

№ 304

**Об утверждении Политики в отношении обработки и защиты  
персональных данных и Положения об обработке  
информации ограниченного доступа в Администрации  
Сосновского муниципального района Нижегородской  
области**

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях обеспечения надежной защиты информации ограниченного доступа в Администрации Сосновского муниципального района Нижегородской области, Администрация Сосновского муниципального района постановляет:

1. Утвердить «Политику в отношении обработки и защиты персональных данных» в Администрации Сосновского муниципального района Нижегородской области.

2. Утвердить «Положения об обработке информации ограниченного доступа», уточняющего правила обработки и защиты персональных данных в Администрации Сосновского муниципального района Нижегородской области.

3. Ответственность за исполнение настоящего постановления возложить на заведующего информационным сектором управления делами Администрации Сосновского муниципального района Нижегородской области (Афонин Д.С.).

4. Контроль за исполнением настоящего постановления возложить на управляющего делами Администрации Сосновского муниципального района Нижегородской области (Е.В. Федина).

Глава местного самоуправления  
Сосновского муниципального района

А.С.Зимин

Утверждена  
постановлением Администрации  
Сосновского муниципального района  
Нижегородской области  
от 18.09.2020 № 304

**Политика  
в отношении обработки и защиты персональных данных в Администрации  
Сосновского муниципального района Нижегородской области**

**I. Общие положения**

1.1. Настоящий документ определяет политику Администрации Сосновского муниципального района Нижегородской области в отношении обработки и защиты персональных данных (далее – Политика) и действует в отношении всех персональных данных, обрабатываемых в Администрации Сосновского муниципального района Нижегородской области (далее – Администрация).

1.2. Настоящая Политика определяет категории персональных данных, обрабатываемых в Администрации, категории субъектов, персональные данные которых обрабатываются в Администрации, цели, принципы, механизм и условия обработки персональных данных, а также меры защиты персональных данных, направленные на обеспечение выполнения Администрацией как оператором персональных данных обязанностей, предусмотренных действующим законодательством.

1.3. Обработка персональных данных в Администрации осуществляется в соответствии с:

- 1) Конституцией Российской Федерации;
- 2) Гражданским кодексом Российской Федерации;
- 3) Трудовым кодексом Российской Федерации;
- 4) Налоговым кодексом Российской Федерации;
- 5) Федеральным законом от 21 ноября 1996 года № 129-ФЗ «О бухгалтерском учете»;
- 6) Федеральным законом от 15 декабря 2001 года № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- 7) Федеральным законом от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации»;
- 8) Федеральным законом от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- 9) Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- 10) Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 11) Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- 12) Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- 13) Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- 14) постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 15) постановлением Правительства Российской Федерации от 21 марта 2012 года № 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»;

16) постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

17) приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

18) приказом Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

19) приказом ФСБ России от 10.07.2014 №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

20) методическими рекомендациями по применению приказа Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденными Роскомнадзором 13 декабря 2013 года;

21) правилами внутреннего трудового распорядка Администрации;

22) иными нормативными правовыми актами, регулирующими процесс обработки и защиты персональных данных.

1.4. Настоящая Политика не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов, имеющих статус архивных документов в соответствии с действующим законодательством об архивном деле в Российской Федерации.

1.5. Положения настоящей Политики являются обязательными для исполнения всеми сотрудниками Администрации.

## **II. Категории обрабатываемых персональных данных**

2.1. В Администрации обрабатываются персональные данные, которые не относятся в соответствии с действующим законодательством к специальным и биометрическим категориям персональных данных, а также персональные данные специальной категории.

2.2. Администрация не обрабатывает персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной (частной) жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности.

2.3. Обработка специальной категории персональных данных субъекта (сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения им трудовых функций) осуществляется Администрацией в соответствии с п. 2.3 ч. 2 ст. 10 Федерального закона № 152-ФЗ, а в соответствии с п. 3 ч. 2 ст. 10 Федерального закона № 152-ФЗ осуществляется обработка сведений о состоянии здоровья в случаях, когда 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.

### **III. Категории субъектов персональных данных**

Под категориями субъектов, персональные данные которых обрабатываются в Администрации, понимаются следующие категории:

1) сотрудники Администрации, замещающие или ранее замещавшие в Администрации должности муниципальной службы и должности, не отнесенные к должностям муниципальной службы;

2) близкие родственники сотрудников Администрации;

3) претенденты на замещение должностей в Администрации или должностей руководителей подведомственных Администрации организаций (предприятий, учреждений), претендующие или ранее претендовавшие на замещение данных должностей в рамках: проведения конкурса на замещение вакантной должности муниципальной службы; проведения мероприятий по замещению должности, не отнесенной к муниципальной службе; перевода с другого места работы (службы); проведения мероприятий по включению в кадровый резерв;

4) руководители подведомственных Администрации организаций (предприятий, учреждений), замещающие или ранее замещавшие данную должность;

5) практиканты (стажеры), проходящие или ранее проходившие практику (стажировку) в Администрации;

6) контрагенты, к которым относятся поставщики (исполнители, подрядчики), имеющие или ранее имевшие с Администрацией договорные отношения;

7) заявители, к которым относятся граждане, осуществляющие или ранее осуществлявшие обращение в Администрацию, в том числе с целью личного приема;

8) граждане, обратившиеся в рамках системы обеспечения вызова экстренных оперативных служб по единому номеру «112» в Нижегородской области / в рамках иных систем обеспечения общественной безопасности, а также граждане, в отношении которых поступили обращения.

9) граждане, принимающие участие в совещаниях, комиссиях, советах и пр. при Администрации района.

### **IV. Цели обработки персональных данных**

Обработка персональных данных в Администрации осуществляется в целях:

1) исполнения функций, полномочий и задач возложенных на Администрацию (рассмотрение обращений заявителей в соответствии с требованиями действующего законодательства, в том числе в рамках личного приема граждан; заключение и исполнение гражданско-правовых договоров между контрагентами и Администрацией; обязательное опубликование или раскрытие персональных данных субъектов в соответствии с действующим законодательством; исполнение запросов федеральных и региональных ведомств; обработка обращений граждан в рамках системы обеспечения вызова экстренных оперативных служб по единому номеру «112» в Нижегородской области, а также в рамках иных систем обеспечения общественной безопасности);

2) реализации служебных и трудовых отношений (принятие решения о трудоустройстве граждан в Администрацию или на должности руководителей подведомственных Администрации организаций (предприятий, учреждений); исполнение требований трудового, налогового и пенсионного законодательства Российской Федерации; ведение бухгалтерского учета);

3) координация деятельности подведомственных Администрации организаций (предприятий, учреждений).

### **V. Механизм обработки персональных данных**

5.1.В Администрации осуществляется смешанная обработка персональных данных как с применением средств вычислительной техники, в информационных

системах персональных данных, так и без использования средств автоматизации.

5.2.В Администрации не производится трансграничная передача персональных данных за исключением случаев защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных при невозможности получения от него согласия в письменной форме на такую передачу, и при условии, что субъект персональных данных является сотрудником Администрации.

## **VI. Принципы и условия обработки персональных данных**

6.1.Обработка персональных данных осуществляется в Администрации с соблюдением следующих принципов:

- 1) обработка осуществляется на законной и справедливой основе;
- 2) обработка ограничивается достижением конкретных, заранее определенных и законных целей;
- 3) обрабатывается тот состав персональных данных и в том объеме, которые отвечают заявленным целям обработки;
- 4) обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается;
- 5) объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой, не допускается;
- 6) при обработке персональных данных обеспечивается их точность, достаточность и в необходимых случаях актуальность по отношению к целям обработки, принимаются меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;
- 7) хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, с соблюдением законодательно определенных требований к обработке и защите персональных данных;
- 8) в случае отзыва субъектом согласия на обработку его персональных данных, а также по достижении целей их обработки или в случае подтверждения факта их неправомерной обработки Администрация прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Администрации);
- 9) обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки, истечению срока обработки, отзыва согласия субъекта персональных данных на обработку, при ликвидации Администрации или в случае утраты необходимости в обработке персональных данных, если иное не предусмотрено действующим законодательством;
- 10) при принятии решений, затрагивающих интересы субъекта персональных данных, Администрация не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

6.2.Лица, получившие от Администрации доступ к персональным данным, обязаны обеспечить их конфиденциальность.

6.3.В Администрации обрабатываются персональные данные субъекта с получением согласия на обработку в случаях, когда его получение в соответствии с действующим законодательством является обязательным условием обработки. Согласие субъекта может быть дано им или его законным представителем (наследником) в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом № 152-ФЗ. С учетом положений действующего законодательства согласие может быть дано в письменной либо электронной форме, оформлено как в виде отдельного документа, так и закреплено в тексте договора (контракта), если это применимо и ничему не противоречит. В случае отзыва согласия на обработку персональных данных Администрация вправе продолжить их обработку без согласия только при наличии оснований, определенных действующим законодательством.

6.4.Администрация несет обязанность предоставить доказательство получения согласия на обработку персональных данных или доказательство наличия законодательно определенных оснований, когда такое согласие не требуется.

6.5.Администрация при обработке и защите персональных данных соблюдает законодательно установленные права субъектов персональных данных, а также разъясняет им порядок защиты их прав и законных интересов, и предоставляет возможность заявить возражения. Сведения предоставляются субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам.

6.6.Все сотрудники Администрации знакомятся под роспись с нормативными правовыми и локальными актами (организационно-распорядительными документами), устанавливающими правила обработки и защиты персональных данных, а также об их правах и обязанностях в этой области.

## **VII. Сведения о третьих лицах, участвующих в обработке персональных данных**

7.1.В целях реализации служебных и трудовых отношений Администрация предоставляет персональные данные определенных категорий субъектов в территориальные налоговые службы (инспекции), пенсионные фонды, органы статистики, органы (фонды) социального страхования, военные комиссариаты, профсоюзные органы, банковские организации. В целях осуществления Администрацией возложенных на нее функций Администрация предоставляет персональные данные определенных категорий субъектов в федеральные и региональные ведомства. Контрольно-надзорным органам, в том числе органам прокуратуры, правоохранительным органам, органам безопасности, государственным инспекциям труда Администрация предоставляет доступ к персональным данным только в пределах их компетенции, в том объеме и для осуществления только тех целей, которые необходимы им для реализации функций, установленных для них действующим законодательством Российской Федерации.

7.2.Передача персональных данных субъекта в коммерческих целях не осуществляется.

7.3.Администрация вправе поручить обработку персональных данных субъектов третьим лицам с соблюдением требований действующего законодательства, предъявляемых к обработке и защите персональных данных.

## **VIII. Защита персональных данных при их обработке.**

### **Меры, направленные на обеспечение выполнения Администрацией обязанностей, предусмотренных статьями 18.1 и 19 Федерального закона № 152-ФЗ**

8.1.При обработке персональных данных Администрация принимает с учетом требований действующего законодательства все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных. Администрация самостоятельно определяет состав и перечень указанных мер, необходимых и достаточных для обеспечения выполнения ей требований действующего законодательства в области обработки и защиты персональных данных.

8.2.Обеспечение защиты персональных данных в Администрации достигается следующими способами:

1) применением предусмотренных нормативными правовыми актами в области обработки и защиты персональных данных необходимых правовых, организационных и технических мер по обеспечению безопасности персональных

данных при их обработке, в том числе в информационных системах персональных данных;

2) назначением в установленном порядке лица, ответственного за организацию обработки персональных данных в Администрации, администраторов и администраторов безопасности информационных систем персональных данных;

3) утверждением Положения об обработке информации ограниченного доступа, уточняющего правила обработки и защиты персональных данных в Администрации;

4) ознакомлением лиц, указанных в подпункте 2 настоящего пункта Политики, и сотрудников Администрации, имеющих доступ к персональным данным в целях их обработки, к информационным системам персональных данных и их компонентам, с положениями настоящей Политики, действующим законодательством и иными локальными актами по вопросам обработки и защиты персональных данных;

5) осуществлением контроля соответствия обработки и защиты персональных данных в Администрации требованиям действующего законодательства, настоящей Политики и иных локальных актов, а также оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных, в том числе до ввода информационных систем персональных данных в эксплуатацию;

6) осуществлением контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

7) оценкой вреда (возможных последствий), который может быть причинен субъектам персональных данных в случае нарушения действующего законодательства в области обработки и защиты персональных данных, соотношение указанного вреда и принимаемых Администрацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством, настоящей Политикой и иными локальными актами;

8) установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

9) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

10) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

11) учетом носителей персональных данных;

12) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

13) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

14) выполнением требований, определенных постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», при обработке персональных данных, осуществляемой без использования средств автоматизации;

15) осуществлением обезличивания персональных данных, обрабатываемых в информационных системах персональных данных, в случаях, установленных действующим законодательством в соответствии с требованиями и методами, определенными уполномоченным органом по защите прав субъектов персональных данных;

16) уведомлением в соответствии с Федеральным законом № 152-ФЗ уполномоченного органа по защите прав субъектов персональных данных об обработке либо намерении осуществлять обработку персональных данных в Администрации.

8.3. Обязанности и ответственность лиц, указанных в подпункте 2 пункта 8.2 настоящей Политики, определяются локальными актами Администрации.

8.4. В случае появления обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые невозможно предвидеть и предотвратить, сотрудники Администрации, имеющие доступ к персональным данным, обязаны принять все возможные меры по недопущению нарушения прав субъектов персональных данных.

#### **IX. Ответственность за нарушение положений настоящей Политики**

Администрация и должностные лица Администрации, участвующие в обработке персональных данных субъектов, несут ответственность в соответствии с действующим законодательством Российской Федерации за несоблюдение положений настоящей Политики и действующего законодательства в сфере обработки и защиты персональных данных.



Утверждено  
постановлением Администрации  
Сосновского муниципального района  
Нижегородской области  
от 18.09.2020 № 304

**Положение**  
**об обработке информации ограниченного доступа в Администрации**  
**Сосновского муниципального района Нижегородской области**  
(далее – Положение)

**I. Общие положения**

1.1. Настоящее Положение определяет (уточняет) основные правила обработки и обеспечения безопасности информации ограниченного доступа (распространения), не отнесенной к государственной тайне (далее – информация ограниченного доступа), в Администрации Сосновского муниципального района Нижегородской области (далее – Администрация), а также раскрывает Политику в отношении обработки и защиты персональных данных, утвержденную Администрацией.

1.2. Действие настоящего Положения распространяется на любое действие (операцию) или совокупность действий (операций), совершаемых с информацией ограниченного доступа с использованием средств вычислительной техники (автоматизации) или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

1.3. Настоящее Положение является обязательным для исполнения всеми сотрудниками Администрации, в т.ч. сотрудниками, имеющими доступ к информации ограниченного доступа.

**II. Защищаемая информация**

К информации ограниченного доступа относятся:

1) персональные данные сотрудников Администрации, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях, а также персональные данные иных субъектов, чьи данные обрабатываются в Администрации;

2) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна): сведения, содержащиеся в обрабатываемых документах с пометкой «Для служебного пользования», в части не содержащей сведения, составляющие государственную тайну;

3) сведения ограниченного доступа, образующиеся в деятельности Администрации и ограничение на распространение которых определяется служебной необходимостью и (или) требованиями действующего законодательства (за исключением сведений, которые не могут быть отнесены к информации ограниченного распространения):

- сведения о системе защиты защищаемой информационной системы (государственная информационная система; информационная система персональных данных; иная информационная система, обрабатываемая информация в которой подлежит защите в соответствии с требованиями действующего законодательства и по решению Администрации), включая данные модели угроз безопасности информации, модели нарушителя безопасности информации, проектного (эксплуатационного) решения на систему безопасности защищаемой информационной системы (далее – ИС), технического паспорта ИС

(сегмента ИС);

- сведения о применяемых средствах защиты информации (СрЗИ): настройки, конфигурация, размещение;
- парольная, ключевая и аутентифицирующая информация;
- перечень помещений и мест обработки и хранения информации ограниченного доступа;
- сведения об информационно-телекоммуникационных сетях, используемых для передачи информации ограниченного доступа: архитектура, настройки;
- сведения о пользовательской (серверной) ИТ-инфраструктуре, задействованной в процессах обработки и хранения информации ограниченного доступа: настройки, конфигурация, разграничение доступа;
- сведения о резервном копировании и восстановлении информации;
- данные регистрируемых событий безопасности;
- сведения о специальном программном обеспечении ИС: настройки, конфигурация, разграничение доступа.

4) сведения ограниченного доступа, обрабатываемые в ИС и ограничение на распространение, которых определяется служебной необходимостью и (или) требованиями действующего законодательства;

5) сведения ограниченного доступа, ограничение на распространение которых наложено другими лицами (организациями) и обрабатываемые в Администрации.

### **III. Конфиденциальность**

3.1.К информации ограниченного доступа применяется режим соблюдения ее конфиденциальности.

3.2.Все документы и сведения, содержащие информацию ограниченного доступа, являются конфиденциальными. Меры конфиденциальности распространяются на материальные носители, содержащие информацию ограниченного доступа.

3.3.Режим конфиденциальности персональных данных снимается в случае их обезличивания и по истечении срока их хранения, и не действует в отношении общедоступных персональных данных.

### **IV. Организация безопасной обработки защищаемой информации**

4.1.Обработка и защита информации ограниченного доступа в Администрации осуществляется в соответствии с требованиями действующего законодательства.

4.2.Администрация при обработке информации ограниченного доступа принимает необходимые правовые, организационные и технические меры ее защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении нее, что в совокупности представляет собой систему защиты, направленную на обеспечение и поддержание требуемого уровня безопасности информации.

4.3.В целях обеспечения безопасности информации ограниченного доступа защите подлежат информационные (автоматизированные) системы, содержащие защищаемую информацию, информационно-телекоммуникационные сети, используемые для передачи защищаемой информации, инженерная и информационно-телекоммуникационная инфраструктура (ИТ-инфраструктура) и помещения, задействованные в процессах обработки и хранения защищаемой информации, носители защищаемой информации и объекты хранения таких носителей, а также средства изготовления и размножения защищаемых документов.

4.4.В Администрации для всех лиц, участвующих в обработке или обеспечении безопасности информации ограниченного доступа, обеспечен доступ к актуальным версиям организационно-распорядительных документов Администрации, регулирующих вопрос обработки или защиты указанной

информации.

4.5.Администрацией проводится внутренний контроль (аудит) выполнения в Администрации требований надлежащей обработки и защиты информации ограниченного доступа с целью определения соответствия обработки такой информации требованиям установленных норм и правил, и оценки эффективности применяемых мер. Внутренний контроль (аудит) осуществляется на плановой и (или) внеплановой основах. В части контроля обработки и защиты персональных данных применяются Правила проведения мероприятий по внутреннему контролю обработки и защиты персональных данных, утвержденные Администрацией.

4.6.Создание, модернизация и ликвидация ИС проводятся в соответствии с требованиями действующего законодательства подразделением Администрации, занимающимся ее созданием (модернизацией, внедрением). В случае ликвидации проводятся мероприятия по уничтожению или передаче (если необходимо) информации в другие системы, на другие носители информации.

4.7.В ИС используются средства защиты информации (СЗИ), прошедшие процедуру оценки соответствия (сертификацию) требованиям действующего законодательства в области защиты информации.

4.8.Базы данных информации ограниченного доступа размещаются Администрацией на технических (вычислительных) площадках, находящихся на территории Российской Федерации.

4.9.Перед началом обработки информации ограниченного доступа сотрудники Администрации, работающие с такой информацией (имеющие доступ):

1) проходят инструктаж (обучение) правилам обработки и защиты информации ограниченного доступа в Администрации, знакомятся с действующим законодательством и организационно-распорядительными документами Администрации, регламентирующими данный вопрос. Инструктаж проводится уполномоченными сотрудниками Администрации в рамках компетенции (полномочий) при: приеме на работу, переводе на другую должность, изменении функционала; изменении законодательства и правовых актов Администрации в области обработки и защиты информации ограниченного доступа; выявлении серьезных нарушений в ходе контрольных проверок; вводе в эксплуатацию новых или модернизации существующих защищаемых ИС / СЗИ. Обучение в виде повышения квалификации (переподготовки) проводится в случае необходимости глубокого изучения требований действующего законодательства в области обработки и защиты информации ограниченного доступа. Сведения о проведенном инструктаже (обучении) фиксируются в Журнале учета инструктажа и обучения по вопросам обеспечения информационной безопасности, который ведется ответственным лицом за защиту персональных данных в Администрации;

2) подписывают Соглашение о неразглашении защищаемой информации (Соглашение о неразглашении персональных данных);

3) подписывают обязательство о прекращении обработки защищаемой информации (обязательство о прекращении обработки персональных данных), по которому они обязуются прекратить обработку информации ограниченного доступа в случае расторжения с ними служебного контракта (трудового договора).

4.10.Сотрудники Администрации, имеющие доступ к информации ограниченного доступа, обязуются:

- знать и выполнять требования действующего законодательства и организационно-распорядительных документов Администрации, регламентирующих порядок обработки и защиты информации ограниченного доступа;

- не разглашать и не использовать (в т.ч. после увольнения из Администрации) в личных и коммерческих целях, целях, не связанных со служебной необходимостью, информацию ограниченного доступа, ставшую известной в связи с исполнением должностных обязанностей;

- не использовать информацию ограниченного доступа для подготовки

открытых публикаций, докладов и т.п.;

- принимать меры, направленные на предотвращение несанкционированного доступа, распространения, разглашения, изменения, уничтожения и блокирования информации ограниченного доступа;

- применять индивидуальные пароли к электронным папкам (архивам), содержащим файлы с информацией ограниченного доступа;

- немедленно ставить в известность своего непосредственного руководителя и уполномоченных сотрудников Администрации в соответствии с компетенцией об утрате или недостатке носителей, содержащих информацию ограниченного доступа, ключей (в т.ч. электронных) от помещений (сейфов, шкафов), в которых обрабатывается (хранится) информация ограниченного доступа, утечке конфиденциальных сведений, о фактах, которые могут привести к несанкционированному распространению (разглашению) защищаемой информации, о причинах и условиях утечки, о попытках посторонних лиц получить от сотрудника Администрации информацию ограниченного доступа, а также сведения, способствующие получению защищаемой информации.

4.11. При работе с бумажными носителями информации ограниченного доступа сотрудники Администрации должны соблюдать Правила работы с бумажными носителями защищаемой информации, утвержденные постановлением Администрации, при работе с машинными носителями информации ограниченного доступа – Правила работы с машинными носителями, Правила работы с техническими средствами и Правила работы со средствами защиты информации, утвержденные правовым актом Администрации.

4.12. Все сотрудники Администрации должны соблюдать Порядок доступа в помещения и Правила реагирования на инциденты информационной безопасности, утвержденные правовым актом Администрации.

## **V. Уполномоченные сотрудники**

5.1. Общее руководство, координацию и контроль за выполнением требований надлежащей обработки и защиты информации ограниченного доступа в Администрации осуществляет ответственный за организацию защиты информации, не отнесенной к государственной тайне (далее – ответственный за организацию ЗИ), в части персональных данных – ответственный за организацию обработки персональных данных. Ответственный за организацию ЗИ назначается из числа сотрудников Администрации. Ответственный за организацию обработки персональных данных назначается из числа сотрудников Администрации.

5.2. За поддержание безопасного функционирования (защиту) ИС, защиту содержащейся в ней информации, а также за обеспечение безопасности персональных данных (при их обработке в ИС) отвечает администратор безопасности ИС. Администратор назначается из числа сотрудников Администрации, которые обладают навыками и знаниями по управлению СЗИ, предпочтительно – администраторов безопасности ИТ-инфраструктуры Администрации. Администратор осуществляет свои функции в соответствии с Инструкцией администратора безопасности информационной системы, утвержденной правовым актом Администрации.

5.3. За создание / ввод в эксплуатацию / эксплуатацию / модернизацию / вывод из эксплуатации ИС, а также за организацию работы пользователей со специальным программным обеспечением (СПО) ИС, контроль правильной эксплуатации СПО ИС и функционирование ИТ-инфраструктуры (локальной вычислительной сети) Администрации, используемой ИС, а также за организацию работы с машинными носителями и техническими средствами Администрации, используемыми ИС, и их функционирование отвечает администратор ИС:

- 1) Администратор ИС, ответственный за функционирование ИТ-инфраструктуры (локальной вычислительной сети) Администрации, используемой

ИС, а также за организацию работы с машинными носителями и техническими средствами Администрации, используемыми ИС, и их функционирование именуется администратором ИС с функциями локального администратора и осуществляет свои функции в соответствии с Инструкцией локального администратора, утвержденной правовым актом Администрации, в части касающейся;

2) Администратор ИС, ответственный за организацию жизненного цикла ИС, за организацию работы пользователей с СПО ИС и контроль правильной эксплуатации СПО ИС, осуществляет свои функции в соответствии с Инструкцией администратора информационной системы, утвержденной правовым актом Администрации. Администратор назначается из числа сотрудников Администрации, которые непосредственно работают в ИС или в чьем ведении находятся вопросы ее жизненного цикла (использования).

Администратором ИС может быть назначено одно или несколько лиц.

5.4.3а функционирование ИТ-инфраструктуры (локальной вычислительной сети) Администрации, участвующей в обработке и (или) хранении информации ограниченного доступа (не в рамках ИС), организацию работы с машинными носителями и техническими средствами Администрации, применяемыми для работы с защищаемой информацией (не в рамках ИС), и их функционирование отвечает локальный администратор. Администратор назначается из числа сотрудников Администрации, которые обладают навыками и знаниями по управлению компьютерным оборудованием. Администратор осуществляет свои функции в соответствии с Инструкцией локального администратора, утвержденной правовым актом Администрации.

5.5.3а поддержание безопасного функционирования (защиту) ИТ-инфраструктуры (локальной вычислительной сети) Администрации, участвующей в обработке и (или) хранении информации ограниченного доступа (не в рамках ИС), организацию безопасной работы (защиты) с машинными носителями и техническими средствами Администрации, применяемыми для работы с защищаемой информацией (не в рамках ИС), отвечает администратор безопасности ИТ-инфраструктуры Администрации. Администратор назначается из числа сотрудников Администрации, которые обладают навыками и знаниями по управлению СЗИ. Администратор осуществляет свои функции в соответствии с Инструкцией администратора безопасности ИТ-инфраструктуры, утвержденной правовым актом Администрации.

## **VI. Доступ к защищаемой информации и информационным системам**

6.1. Доступ к информации ограниченного доступа и ИС предоставляется сотрудникам Администрации и третьим лицам, не входящим в штатную структуру Администрации, в связи со служебной (производственной) необходимостью, в объеме, необходимом для выполнения ими должностных обязанностей (функций), с соблюдением принципа предоставления минимально необходимых привилегий и при подписании Соглашения о неразглашении защищаемой информации (Соглашения о неразглашении персональных данных), типовая форма которого утверждена правовым актом Администрации.

6.2. Третьим лицам доступ к информации ограниченного доступа предоставляется при наличии договорных отношений (соглашений) с Администрацией, разрешающих (подразумевающих) доступ к информации ограниченного доступа, или в случаях, предусмотренных действующим законодательством, и на ограниченный период времени, который может определяться сроком действия договорных обязательств, если действующим законодательством не установлено иное.

6.3. Факт доступа третьих лиц к персональным данным фиксируется в Журнале учета доступа к персональным данным, который ведется ответственным специалистом Администрации.

6.4. Факт доступа третьих лиц к ИС фиксируется в Журнале учета доступа к информационным системам, который ведется Администрацией.

6.5. Необходимость предоставления, изменения и (или) ликвидации прав доступа (далее – пересмотр прав доступа) сотрудника Администрации к информации ограниченного доступа и ИС определяется при его приеме на работу, при изменении его должностных обязанностей (функций) и при его увольнении; необходимость пересмотра прав доступа для третьего лица определяется характером договорных отношений (соглашений) и сроком их действия, а также действующим законодательством.

6.6. Необходимость пересмотра прав доступа к информации ограниченного доступа и ИС определяется и своевременно доводится до уполномоченного сотрудника Администрации руководителем структурного подразделения Администрации, в чьем подчинении (под чьим контролем) находится сотрудник (третье лицо), которому необходимо пересмотреть права доступа. В части доступа к персональным данным и информационным системам персональных данных – до ответственного за организацию обработки персональных данных, в части доступа к ИС и содержащейся в ней информации – до администратора ИС и администратора безопасности ИС в соответствии с компетенцией. Уполномоченными сотрудниками Администрации организуется необходимая работа по пересмотру прав доступа.

6.7. Доступ сотрудника Администрации (третьего лица) к информации ограниченного доступа и ИС может быть временно заблокирован на период проведения разбирательства в случае подозрения на злоупотребление сотрудником Администрации (третьим лицом) полномочиями, несанкционированную (неправомерную) обработку им информации ограниченного доступа или несанкционированное использование им ИС.

## **VII. Условия и порядок сбора (получения) персональных данных**

7.1. Все персональные данные субъекта сотрудники Администрации получают у него самого. Если персональные данные субъекта могут быть получены только у третьей стороны, то субъект уведомляется об этом заранее, и от него получается письменное согласие. Ответственный специалист получает подтверждение от третьего лица, передающего персональные данные о том, что они передаются с согласия субъекта.

7.2. В установленных действующим законодательством случаях ответственный специалист сообщает субъекту о целях, предполагаемых источниках и способах получения его персональных данных, а также о характере подлежащих получению данных и последствиях его отказа дать письменное согласие на получение и (или) предоставление данных (последствиях отказа предоставить свои персональные данные).

7.3. Сотрудники Администрации предоставляют сотрудникам сектора учета и отчетности управления делами Администрации и сотрудникам организационно – правового отдела управления делами Администрации, имеющим доступ к их персональным данным, достоверные сведения о себе и в срок, не превышающий 5 (пяти) рабочих дней, сообщают об изменении своих данных с приложением при необходимости подтверждающих документов. Сотрудники сектора учета и отчетности Администрации и сотрудники организационно – правового отдела управления делами Администрации проверяют при необходимости и наличии законных оснований достоверность сведений, сверяя предоставленные данные с имеющимися у них документами (сведениями) или направляя запросы.

7.4. При поступлении на работу (службу) в Администрацию субъект заполняет анкету по утвержденной форме (при ее заполнении в строгом соответствии с записями, которые содержатся в его личных документах, заполняются все графы анкеты, на все вопросы даются полные ответы, не допускается исправлений или зачеркиваний, прочерков, помарок) и дает согласие на обработку своих

персональных данных на период принятия решения о приеме либо отказе в приеме на работу (службу). Получение согласия является обязательным условием при направлении Администрацией запросов в иные организации, в том числе, по прежним местам работы (службы) субъекта, для уточнения или получения о нем информации.

### **VIII. Обработка персональных данных**

8.1. Обработка персональных данных осуществляется в случаях и в сроки, определенные действующим законодательством, Политикой в отношении обработки и защиты персональных данных, утвержденной правовым актом Администрации, и настоящим Положением.

8.2. В предусмотренных действующим законодательством случаях Администрация уведомляет субъекта о совершенных операциях над его персональными данными по типовой форме, утвержденной Администрацией.

8.3. При поручении обработки персональных данных третьим лицам такие данные не сообщаются третьей стороне без письменного согласия самого субъекта, за исключением случаев, предусмотренных действующим законодательством.

8.4. Обработка персональных данных субъектов может осуществляться без их согласия в случаях, установленных Федеральным законом № 152-ФЗ, в т.ч., если:

1) обработка персональных данных ведется при осуществлении пропускного режима (режима допуска) на территорию помещений Администрации, при условии, что организация пропускного режима (режима допуска) осуществляется Администрацией самостоятельно;

2) обработка персональных данных близких родственников сотрудников Администрации осуществляется в объеме, предусмотренном Formой Т-2, анкетой, справкой о доходах либо в случаях, установленных действующим законодательством (оформление социальных выплат, льгот и пр.);

3) обрабатываются данные уволенных сотрудников Администрации в рамках исполнения нормы подпункта 5 пункта 3 статьи 24 Налогового кодекса Российской Федерации, в котором установлена обязанность налоговых агентов (работодателей) в течение 4 (четырёх) лет обеспечивать сохранность документов, необходимых для исчисления, удержания и перечисления налога, и в рамках выполнения требований статьи 17 Федерального закона от 21 ноября 1996 года № 129-ФЗ «О бухгалтерском учете», в которой определяется, что организации обязаны хранить бухгалтерскую документацию в течение сроков, устанавливаемых в соответствии с правилами организации государственного архивного дела, но при этом минимальный срок хранения не может быть менее 5 (пяти) лет;

4) обрабатываются данные претендентов на замещение должностей в случаях: если от имени субъекта действует кадровое агентство, с которым субъект заключил соответствующий договор; если субъект самостоятельно разместил свое резюме в сети «Интернет» и оно стало доступно неограниченному кругу лиц; если типовая форма анкеты субъекта реализована Администрацией в электронной форме на сайте Администрации, где согласие на обработку персональных данных подтверждается субъектом путем проставления отметки в соответствующем поле.

8.5. В случае получения резюме субъекта по каналам электронной почты или факсимильной связи Администрация дополнительно проводит мероприятия, направленные на подтверждение факта направления резюме самим субъектом (осуществляет обратную связь посредством электронной почты) и получение согласия на обработку его персональных данных (приглашает субъекта на личную встречу). В случае невозможности получения согласия (отказа субъекта приехать на личную встречу или подписать необходимый документ) Администрация прекращает обработку персональных данных и уничтожает полученное резюме. В случае, если резюме не заинтересовало Администрацию или по резюме, составленному в произвольной форме, невозможно однозначно определить физическое лицо,

которое его направило, указанное резюме подлежит уничтожению в день поступления. В случае отказа субъекту в приеме на работу (службу) сведения, им предоставленные, уничтожаются в течение 30 (тридцати) дней.

8.6. Если персональные данные получены не от субъекта, Администрация, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ, до начала их обработки предоставляет субъекту сведения, предусмотренные Федеральным законом № 152-ФЗ.

8.7. При осуществлении автоматизированной обработки персональных данных:

1) на основании полученных данных проверяется наличие информации о субъекте в электронных учетных (учетно-отчетных) формах или ИС. Если субъект отсутствует в таких формах / ИС, то полная информация о нем заносится после получения его согласия, а в случае наличия информации о субъекте – сверяются данные с ранее предоставленными и при необходимости вносятся соответствующие изменения;

2) не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в электронных учетных (учетно-отчетных) формах или ИС, конкретному субъекту.

8.8. При осуществлении неавтоматизированной обработки персональных данных соблюдается порядок, аналогичный указанному в пункте 6.7 настоящего Положения, и уточнение персональных данных 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 данными.

## **IX. Хранение защищаемой информации**

9.1. Хранение персональных данных в Администрации осуществляется в случаях и в сроки, установленные действующим законодательством, но не дольше, чем этого требуют цели обработки персональных данных, если срок их хранения не установлен действующим законодательством, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект.

9.2. Сроки хранения документов, содержащих персональные данные сотрудников Администрации, установлены в соответствии с «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утв. Приказом Росархива от 20 декабря 2019 г. N 236.

9.3. Личные дела сотрудников Администрации хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела муниципальных служащих Администрации, уволенных со службы (за исключением перевода), хранятся в течение 10 (десяти) лет со дня увольнения со службы, после чего передаются в архив. Сохранность личных дел сотрудников Администрации обеспечивает организационно-правовой отдела управления делами Администрации. При переводе муниципального служащего Администрации на должность муниципальной службы в другой орган его личное дело передается по новому месту работы (службы). Если субъект, личное дело которого хранится в архиве, поступит на службу вновь, его личное дело также передается по месту работы.

9.4. Персональные данные субъектов:

1) категории «сотрудники Администрации», «близкие родственники», «практиканты (стажеры)», «руководители подведомственных Администрации организаций», «претенденты на замещение должностей» и «контрагенты», содержащиеся на бумажных носителях, хранятся в специальном шкафу (сейфе), установленном в помещении сектора учета управления и отчетности управления делами Администрации и организационно-правового отдела управления делами



Администрации;

2) категории «сотрудники Администрации» и «контрагенты», содержащиеся на машинных носителях, хранятся на АРМ сотрудников сектора учета и отчетности Администрации или организационно-правовом отделе управления делами Администрации;

3) категории «заявители», содержащиеся на бумажных носителях, хранятся в специальном шкафу (сейфе), установленном в помещении структурного подразделения Администрации ответственного за исполнение заявления (обращения) «заявителя», а содержащиеся на машинных носителях – на АРМ сотрудников структурного подразделения Администрации ответственного за исполнение заявления (обращения) «заявителя».

9.5.В соответствии с «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утв. Приказом Росархива от 20 декабря 2019 г. N 236, в Администрации в рамках сроков, установленных данным документом, также хранятся:

1) документы (списки, обязательства, расписки) лиц, принявших обязательства о неразглашении сведений ограниченного доступа (конфиденциального характера, служебной и коммерческой тайны);

2) документы (заявления работника о согласии на обработку персональных данных, сведения, уведомления) о субъекте персональных данных;

3) локальные нормативные акты (положения, инструкции) о персональных данных работников;

4) документы (акты, заключения, справки, переписка) о состоянии защиты информации в Администрации;

5) распорядительная и эксплуатационно-техническая документация (инструкции, руководства и др.) обслуживающему персоналу и пользователям информации по защите информации;

6) схемы организации криптографической защиты конфиденциальной информации;

7) документы (заявки, отчеты, анализы) по антивирусной защите средств электронно-вычислительной техники;

8) документы (акты, справки, заявки, расчеты, ведомости, журналы учета сдачи и приемки оборудования после ремонта, переписка) о состоянии и проведении ремонтных, наладочных работ технических средств;

9) списки лиц, имеющих допуск к компьютерному оборудованию, к сети;

10) перечни работ по резервному копированию информации.

9.6. Действия с ключами (электронными картами) от кабинетов, хранилищ (сейфы, шкафы и т.п.) фиксируются в соответствующем журнале учета. Ключи (электронные карты) не подлежат несанкционированному копированию (изготовлению дубликатов), не подлежат бесконтрольному нахождению в замках кабинетов, хранилищ и в иных местах, не исключающих несанкционированный доступ к ним. Ключи (электронные карты) подлежат возврату лицом, которому они были выданы, при его увольнении или утрате им прав доступа к хранилищу, кабинету. За сохранность выданных ключей (электронных карт) ответственность несет их пользователь. Выдачу ключей (электронных карт) от хранилищ персональных данных осуществляет ответственный за организацию обработки персональных данных, от хранилищ, содержимое которых имеет отношение к ИТ-инфраструктуре Администрации, – локальный администратор, от хранилищ, содержимое которых имеет отношение к безопасности ИТ-инфраструктуры Администрации, – администратор безопасности ИТ-инфраструктуры Администрации, от хранилищ, содержимое которых имеет отношение к безопасности ИС, – администратор безопасности ИС. Неиспользуемый дубликат (оригинал) ключа (электронной карты) хранится в шкафу (ящике, хранилище (сейфе)), подконтрольном

вышеуказанному уполномоченному лицу, в непросматриваемой упаковке, опечатанной прочной наклейкой по всей длине кромки вскрытия упаковки и удостоверенной подписью (печатью) лица, изготовившего дубликат (получившего оригинал), на месте вскрытия упаковки. Об утери или недостатке ключей (электронных карт) от кабинетов, хранилищ сотрудники Администрации немедленно сообщают вышеуказанному уполномоченному лицу и руководителю Администрации (ответственному за организацию защиты информации, не отнесенной к государственной тайне). При утрате ключа от хранилища замок меняется или переделывается его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от кабинета, хранилища переделать невозможно, то хранилище заменяется. Порядок хранения ключевых и других документов СКЗИ в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает орган криптографической защиты.

9.7.Правила обращения с ключами (электронными картами) от защищаемых помещений определены Порядком доступа в помещения, утвержденным Администрацией.

## **Х. Передача защищаемой информации**

10.1.Передача информации ограниченного доступа осуществляется посредством нарочного, почтовой связи, по каналам электрической связи.

10.2.При передаче информации ограниченного доступа обеспечивается ее конфиденциальность. Передача персональных данных, не носящих характер общедоступных, по телефону, факсимильной связи, электронной почте запрещена. Передача информации ограниченного доступа без использования специальных средств защиты по общедоступным сетям связи запрещена. Защита информации ограниченного доступа от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

10.3.При передаче информации ограниченного доступа через организацию федеральной почтовой связи соблюдаются следующие требования: документы, содержащие информацию ограниченного доступа, вкладываются в конверт, к нему прилагается сопроводительное письмо; на конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией и за незаконное ее разглашение законодательством предусмотрена ответственность; данный конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами.

10.4.Передача (распространение, разглашение) информации ограниченного доступа лицам, не имеющим к ней прав доступа (неопределенному кругу лиц), запрещена.

10.5.Передача информации ограниченного доступа осуществляется на основании договора со стороной, которой осуществляется передача, или письменного запроса, полученного от стороны, которой осуществляется передача (на официальном бланке с указанием на основание получения доступа к информации ограниченного доступа, ее перечень, цель использования, Ф.И.О. и должность лица, которому поручается ее получить), или исполнения функций, возложенных на Администрацию (требований действующего законодательства), или в рамках реализации служебных (трудовых) отношений. Передача информации ограниченного доступа третьим лицам сопровождается подписанием принимающей стороной Соглашения о неразглашении защищаемой информации (Соглашения о неразглашении персональных данных) и Обязательства о прекращении обработки защищаемой информации (Обязательства о прекращении обработки персональных

данных), за исключением законных случаев, когда передача допускается без подписания данных документов.

10.6. При передаче персональных данных сотрудники Администрации:

- 1) проверяют основание на осуществление передачи персональных данных и наличие согласия субъекта на их передачу (если требуется по законодательству);
- 2) не сообщают персональные данные в непредусмотренных целях и случаях;
- 3) не осуществляют передачу персональных данных без права доступа к ним;
- 4) предупреждают лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц подтверждения того, что это правило соблюдено;
- 5) разрешают доступ к персональным данным только уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы им для выполнения их обязанностей или функций;
- 6) передают персональные данные субъекта его представителю, членам его семьи в порядке и при условиях, установленных действующим законодательством, и ограничивают эту информацию только необходимыми данными.

10.7. Согласие сотрудника Администрации на передачу его персональных данных не требуется:

- 1) если их передача необходима в целях предупреждения угрозы жизни и здоровью сотрудника, а получить согласие не представляется возможным;
- 2) если третьи лица оказывают услуги Администрации на основании заключенных договоров, где указаны его данные;
- 3) при передаче данных в территориальные налоговые службы (инспекции), пенсионные фонды, органы статистики, органы (фонды) социального страхования, военные комиссариаты, профсоюзные органы;
- 4) если передача данных сотрудника осуществляется в случаях, связанных с выполнением им должностных обязанностей, в т.ч., при его командировании (в соответствии с Правилами предоставления гостиничных услуг в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 9 октября 2015 г. № 1085, и иными нормативными правовыми актами в сфере транспортной безопасности);
- 5) если персональные данные обрабатываются или передаются в рамках установленных полномочий, мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства, органов и организаций, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом, и иных органов, уполномоченных запрашивать информацию о сотрудниках в соответствии с компетенцией, предусмотренной законодательством (запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации);
- 6) при передаче персональных данных банковским (кредитным) организациям, открывающим и обслуживающим платежные карты для начисления заработной платы, в случаях, если: договор на выпуск банковской карты заключался напрямую с сотрудником и в его тексте предусмотрены положения, предусматривающие передачу Администрацией персональных данных; наличие у Администрации доверенности на представление интересов сотрудника при заключении договора с такой организацией на выпуск банковской карты и ее последующее обслуживание; соответствующая форма и система оплаты труда прописана в трудовом договоре (служебном контракте).

10.8. Администрация обеспечивает ведение Журнала учета выданных персональных данных.

## **XI. Блокирование и разблокирование персональных данных**

11.1.Администрация блокирует персональные данные или обеспечивает их блокирование в сроки, установленные Федеральным законом № 152-ФЗ, в случае:

- 1) выявления неправомерной обработки персональных данных;
- 2) выявления неточных персональных данных;
- 3) получения соответствующего обращения от субъекта (его законного представителя);
- 4) отсутствия возможности уничтожить персональные данные в рамках законодательно установленных сроков.

11.2.Разблокирование персональных данных осуществляется в случаях, предусмотренных Федеральным законом № 152-ФЗ и настоящим Положением. Повторное согласие субъекта на обработку его персональных данных влечет их разблокирование.

11.3.Блокирование (разблокирование) персональных данных проводит сотрудник Администрации, который осуществляет обработку персональных данных субъекта. Если осуществляется блокирование (разблокирование) персональных данных, обрабатываемых в ИС, к проведению работ по блокированию привлекается администратор ИС.

11.4.Разрешение или отказ на блокирование (разблокирование) персональных данных дает ответственный за организацию обработки персональных данных.

11.5.Если обработка персональных данных осуществляется лицом, действующим по поручению Администрации, ответственным за организацию обработки персональных данных организуется необходимая работа по обеспечению их блокирования.

11.6.В случае выявления неправомерной обработки персональных данных субъекта одновременно с принятием решения о блокировании его персональных данных ответственным за организацию обработки персональных данных инициируется проведение проверки персональных данных, заблокированных по причине их неправомерной обработки.

11.7.В случае выявления неточных персональных данных конкретного субъекта сотрудник Администрации, который осуществляет обработку его персональных данных, проводит блокирование данных, относящихся к этому субъекту, или во взаимодействии с ответственным за организацию обработки персональных данных обеспечивает их блокирование, если такое блокирование не нарушает права и законные интересы субъекта или третьих лиц.

11.8.В случае подтверждения факта неточности персональных данных сотрудник Администрации, осуществляющий обработку персональных данных данного субъекта, на основании сведений, представленных субъектом (его законным представителем) либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение и снимает блокирование.

11.9.Блокирование данных конкретного субъекта (если такая необходимость установлена) осуществляется во всех ИС, включая архивы баз данных, содержащих такие персональные данные, во всех материальных носителях, содержащих такие персональные данные (за исключением случаев, когда обработка необходима для уточнения данных).

## **XII. Уничтожение защищаемой информации и ее носителей**

12.1.Уничтожение информации ограниченного доступа проводится в соответствии с Порядком уничтожения защищаемой информации, утвержденным правовым актом Администрации.

12.2.Уничтожение носителей, содержащих информацию ограниченного доступа, проводится в соответствии с Порядком уничтожения носителей защищаемой информации, утвержденным Администрацией.

### **XIII. Обращения субъектов и запросы контрольно-надзорных органов**

13.1. Субъекты, персональные данные которых обрабатываются в Администрации, обращаются в Администрацию в целях и при соблюдении правил обращения, определенных Федеральным законом № 152-ФЗ.

13.2. Администрацией утверждены типовые формы обращений субъектов персональных данных.

13.3. Администрация соблюдает Правила рассмотрения обращений субъектов персональных данных и запросов контрольно-надзорных органов, утвержденных правовым актом Администрации.

### **XIV. Заключительные положения**

14.1. Каждый сотрудник Администрации, допущенный к обработке информации ограниченного доступа и получающий для работы носитель, содержащий такую информацию, несет персональную ответственность за его сохранность и соблюдение безопасности указанной информации при ее обработке.

14.2. В вопросах обработки и защиты информации ограниченного доступа, не урегулированных настоящим Положением, Администрация руководствуется нормами действующего законодательства.

14.3. Если какое-либо из требований Положения в связи с изменением законодательства становится недействительным, это не затрагивает действительности остальных его положений.