АДМИНИСТРАЦИЯ ГОРОДА ЮЖНО-САХАЛИНСКА

ПОСТАНОВЛЕНИЕ

от 21.02.2020 № 489-па

Об обработке персональных данных в администрации города Южно-Сахалинска

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 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», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказами ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказами 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» и от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» и в целях организации работы по обработке персональных данных в администрации города Южно-Сахалинска и обеспечения их безопасности,

администрация города Южно-Сахалинска **постановляет**:

1. Утвердить:

1.1. Правила обработки персональных данных в администрации города Южно-Сахалинска (приложение №1);

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации города Южно-Сахалинска (приложение №2);

1.3. Правила осуществления внутреннего контроля в администрации города Южно-Сахалинска соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (приложение №3);

1.4. Правила работы с обезличенными персональными данными в случае обезличивания персональных данных в администрации города Южно-Сахалинска (приложение №4);

1.5. Перечень информационных систем персональных данных, обрабатываемых в администрации города Южно-Сахалинска (приложение №5);

1.6. Перечень персональных данных, обрабатываемых в администрации города Южно-Сахалинска в связи с реализацией трудовых отношений, а также в связи с оказанием государственных и муниципальных услуг и осуществлением государственных и муниципальных функций (приложение №6);

1.7. Перечень должностей в администрации города Южно-Сахалинска, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных (приложение №7);

1.8. Перечень должностей в администрации города Южно-Сахалинска, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение №8);

1.9. Перечень должностей в администрации города Южно-Сахалинска, доступ к персональным данным которым необходим для выполнения служебных обязанностей (приложение №9);

1.10. Должностную инструкцию ответственного за организацию обработки персональных данных в администрации города Южно-Сахалинска (приложение №10);

1.11. Типовое обязательство сотрудника администрации города Южно-Сахалинска о неразглашении информации, содержащей персональные данные на период исполнения им должностных обязанностей (приложение №11);

1.12. Типовое обязательство сотрудника администрации города Южно-Сахалинска непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить

обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (приложение №12);

1.13. Типовую форму согласия на обработку персональных данных сотрудников администрации города Южно-Сахалинска, иных субъектов персональных данных (приложение №13);

1.14. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение №14);

1.15. Порядок доступа сотрудников администрации города Южно-Сахалинска в помещения, в которых ведется обработка персональных данных (приложение №15);

1.16. Инструкцию по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну и криптоключами к ним (приложение №16);

1.17. Инструкцию ответственного за эксплуатацию средств криптографической защиты информации (приложение №17);

1.18. Политику в отношении обработки персональных данных (приложение №18).

2. Назначить ответственным за организацию обработки персональных данных и ответственным за эксплуатацию средств криптозащиты (далее - СКЗИ) в администрации города Южно-Сахалинска референта Департамента мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска.

3. Руководителям структурных подразделений аппарата и отраслевых функциональных органов администрации города Южно-Сахалинска, осуществляющих обработку персональных данных:

3.1. Обеспечить выполнение требований Правил обработки персональных данных в администрации города Южно-Сахалинска;

3.2. Внести в должностные инструкции сотрудников, уполномоченных на обработку персональных данных, дополнения в части закрепления ответственности, предусмотренной законодательством Российской Федерации за нарушение безопасности обрабатываемых ими персональных данных.

4. Руководителям муниципальных, бюджетных и казенных учреждений, муниципальных унитарных предприятий, входящих в структуру ЕМТС и осуществляющих обработку персональных данных, в срок до 1 апреля 2020 года:

4.1. Назначить ответственных лиц за организацию обработки персональных данных;

4.2. Разработать и утвердить документы об организации работы с персональными данными, аналогичные предусмотренным подпунктами 1.5-1.9

настоящего постановления;

4.3. Внести в должностные инструкции лиц, уполномоченных на обработку персональных данных, дополнения в части закрепления ответственности, предусмотренной законодательством Российской Федерации за нарушение безопасности обрабатываемых ими персональных данных.

5. Руководителям муниципальных, бюджетных и казенных учреждений, муниципальных унитарных предприятий, не входящих в структуру ЕМТС и осуществляющих обработку персональных данных, в срок до 1 апреля 2020 года:

5.1. Назначить ответственных лиц за организацию обеспечения безопасности персональных данных и ответственных лиц за организацию обработки персональных данных;

5.2. Разработать и утвердить документы об организации работы с персональными данными, аналогичные предусмотренным пунктом 1 настоящего постановления;

5.3. Внести в должностные инструкции лиц, уполномоченных на обработку персональных данных, дополнения в части закрепления ответственности, предусмотренной законодательством Российской Федерации за нарушение безопасности обрабатываемых ими персональных данных.

6. Назначить МКУ "Управление делами администрации города Южно-Сахалинска" ответственным за обеспечение безопасности персональных данных в МИС «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска».

7. Признать утратившим силу постановление администрации города Южно-Сахалинска от 26.05.2014 № 926-па «Об обработке персональных данных в администрации города Южно-Сахалинска».

8. Опубликовать настоящее постановление в газете «Южно-Сахалинск сегодня» и разместить на официальном сайте администрации города Южно-Сахалинска.

9. Контроль исполнения постановления администрации города возложить на директора Департамента мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска.

Мэр города С.А.Надсадин

Приложение №1

Утверждены
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Правила
обработки персональных данных
в администрации города Южно-Сахалинска

1. Общие положения

1.1. Администрации города Южно-Сахалинска (далее — Администрация) является оператором, самостоятельно или совместно с другими лицами осуществляющим обработку персональных данных субъектов персональных данных (далее - персональные данные), а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.2. Обработка персональных данных в Администрации осуществляется в целях осуществления муниципальных функций, предоставления государственных и муниципальных услуг и в связи с реализацией трудовых отношений.

2. Правила обработки персональных данных

2.1. Обработка персональных данных в связи с реализацией Администрацией трудовых отношений осуществляется с письменного согласия субъектов персональных данных, которое действует со дня их поступления на работу и на время ее прохождения, как с использованием средств автоматизации, так и без использования таких средств. Обеспечение защиты персональных данных, содержащихся в личных делах субъектов персональных данных, от неправомерного их использования или утраты осуществляется структурным подразделением отвечающим за кадровую политику.

2.2. Персональные данные и иные сведения, содержащиеся в личных делах субъектов персональных данных, относятся к служебной информации ограниченного распространения (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

2.3. Обработка персональных данных для предоставления государственных и муниципальных услуг по запросу заявителя в соответствии с п. 4 ст. 7 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» не требует получения согласия заявителя, как субъекта персональных данных в соответствии с требованиями ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152 - ФЗ).

В случае, если запрос заявителя поступил в Администрацию в форме, не позволяющей достоверно идентифицировать личность заявителя как субъекта персональных данных (по электронной почте, путем заполнения формы на официальном сайте администрации города Южно-Сахалинска или аналогичным способом), Администрация информирует такого заявителя о времени и месте, где он может получить результаты обработки персональных данных по предъявлению документа, удостоверяющего его полномочия субъекта персональных данных.

2.4. При обработке Администрацией персональных данных в целях осуществления муниципальных функций, предоставления государственных и муниципальных услуг и в связи с реализацией трудовых отношений лица, уполномоченные на обработку персональных данных (далее - уполномоченные должностные лица), обязаны соблюдать следующие требования:

2.4.1. объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;

2.4.2. защита персональных данных от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

2.4.3. передача персональных данных не допускается без письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральными законами. В случае, если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных либо отсутствует письменное согласие субъекта персональных данных на передачу его персональных данных, Администрация вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

2.4.4. обеспечение конфиденциальности персональных данных обязательно, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

2.4.5. хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели обработки или в случае утраты необходимости в их

достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется актом, составленным в произвольной форме и утверждаемым руководителем соответствующего структурного подразделения аппарата или отраслевого (функционального) органа Администрации, осуществляющего обработку персональных данных;

2.4.6. опубликование и распространение персональных данных допускается в случаях, установленных законодательством Российской Федерации.

2.5. В целях обеспечения защиты персональных данных субъекты персональных данных вправе:

2.5.1. получать полную информацию о своих персональных данных и способе обработки этих данных (в том числе автоматизированной);

2.5.2. получать свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ ;

2.5.3. требовать внесения необходимых изменений, уничтожения или блокирования персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

2.5.4. обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации

3.1. Обработка персональных данных без использования средств автоматизации осуществляется как на бумажных носителях, так и в электронном виде на материальных носителях информации.

3.2. Неавтоматизированная обработка персональных данных в электронном виде должна осуществляться на съемных материальных носителях информации.

3.3. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на съемных материальных носителях информации необходимо принимать организационные и технические меры, исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

3.4. При обработке персональных данных без использования средств автоматизации уполномоченными должностными лицами не допускается фиксация на одном материальном носителе персональных данных, цели

обработки которых заведомо несовместимы.

3.5. Обработка персональных данных на бумажных носителях осуществляется в соответствии с требованиями, установленными постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.6. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на Администрацию полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

3.6.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Администрации, фамилию, имя, отчество и адрес субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

3.6.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;

3.6.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными не имел возможности доступа к персональным данным других лиц, содержащихся в указанной типовой форме;

3.6.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

3.7. Уничтожение или обезличивание 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).

3.8. Уточнение персональных данных при их обработке без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

4. Правила обработки персональных данных

в информационных системах персональных данных

4.1. Информационные системы персональных данных Администрации входят в состав муниципальной информационной системы «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее — ЕМТС).

4.2. Обязанность по обеспечению защиты информации в ходе эксплуатации аттестованной ЕМТС в соответствии с проектными решениями системы защиты информации ЕМТС и эксплуатационной документации используемой в составе ЕМТС, средств защиты информации, включая управление (администрирование) системой защиты информации ЕМТС осуществляет МКУ «Управление делами администрации города Южно-Сахалинска», как оператор ЕМТС обеспечивающего эксплуатацию аппаратно-технического и программного обеспечения ЕМТС согласно распоряжения Администрации города Южно-Сахалинска от 22.07.19 № 451-р.

4.3. Обработка персональных данных в ЕМТС осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.4. Обработка персональных данных в информационных системах осуществляется после завершения работ по созданию системы защиты персональных данных в информационной системе, ее проверки и оценки соответствия информационной системы персональных данных требованиям безопасности информации.

4.5. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора.

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

4.7. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным.

4.8. Доступ пользователей к персональным данным в информационных системах персональных данных разрешается после обязательного прохождения процедуры идентификации и аутентификации.

4.9. Самостоятельное подключение средств вычислительной техники, применяемой для хранения, обработки или передачи персональных данных, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

4.10. Пользователями информационных систем, администраторами информационной безопасности, должно быть обеспечено:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до первого вице-мэра, руководителя аппарата Администрации;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- учет и соблюдение правил хранения, применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;
- служебные проверки и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.11. В случае выявления нарушений порядка обработки персональных данных уполномоченными должностными лицами принимаются меры по установлению причин таких нарушений и их устранению.

5. Правила допуска и доступа к персональным данным

5.1. Доступ к персональным данным предоставляется:

- уполномоченным должностным лицам, допущенным к обработке персональных данных, в части, касающейся их должностных обязанностей;
- уполномоченным представителям федеральных органов исполнительной власти в установленной сфере деятельности, осуществляющих контрольно-надзорные функции в порядке, установленном законодательством Российской Федерации;
- субъектам персональных данных.

5.2. Фактом ознакомления с разрешением на допуск является подпись уполномоченного должностного лица об ознакомлении со списком должностных лиц, доступ которых к персональным данным необходим для выполнения служебных обязанностей.

5.3. В соответствии с ч.3 ст.6 Федерального закона № 152-ФЗ 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 муниципального контракта, либо на основании нормативно-правового акта Администрации. Лицо, осуществляющее обработку персональных данных по поручению Администрации, обязано соблюдать принципы и правила обработки персональных данных, установленные Федеральным законом № 152-ФЗ.

5.4. В поручении Администрации (договоре, контракте или нормативно-правовом акте) должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, 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 в соответствии со ст. 19 Федерального закона № 152-ФЗ.

5.5. Допуск к персональным данным, в том числе содержащимся в информационных системах персональных данных сторонних организаций, деятельность которых не связана с исполнением функций Администрации, регламентируется законодательством и нормативными правовыми актами Российской Федерации, а также контрактами (договорами, соглашениями) Администрации с операторами соответствующих информационных систем персональных данных.

5.6. Доступ к техническим (программно-техническим) средствам информационных систем персональных данных Администрации предоставляется сторонним организациям, выполняющим работы на

договорной основе, в порядке, установленном требованиями по защите информации.

5.7. Порядок допуска сторонних организаций и/или их представителей к информационным системам персональных данных определяется в муниципальном контракте на выполнение работ (оказание услуг). Решением о допуске является подписанный в установленном порядке муниципальный контракт на выполнение работ (оказание услуг).

5.8. Доступ к персональным данным сторонних организаций осуществляется на основании письменных запросов или письменных соглашений (договоров) сторон об обмене информацией.

5.9. В письменном запросе (соглашении, договоре) должны быть указаны следующие сведения:

- цель получения информации;
- конкретное наименование информации (состав персональных данных);
- способ доступа (предоставления), а также сведения о регистрации организации-заявителя в уполномоченном органе по защите прав субъектов персональных данных.

5.10. При наличии соглашения со сторонней организацией о допуске к персональным данным (предоставлении информации) доступ к персональным данным осуществляется в порядке, указанном в подписанном соглашении (договоре).

5.11. Доступ к персональным данным, в том числе содержащимся в информационных системах персональных данных сторонних организаций, выполняющих работы на договорной основе, осуществляется на основании подписанного договора на оказание услуг, а также настоящих Правил.

5.12. Запрещается передача электронных копий баз (банков) данных, содержащих персональные данные, любым сторонним организациям, за исключением случаев, предусмотренных законодательством Российской Федерации.

Приложение №2

Утверждены
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Правила
рассмотрения запросов субъектов персональных данных или их представителей в администрации города Южно-Сахалинска

1. Общие положения

1.1. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации города Южно-Сахалинска (далее — Администрация) определяют порядок рассмотрения запросов сотрудников Администрации, граждан, претендующих на замещение должностей в Администрации, граждан, персональные данные которых обрабатываются в связи с обращением в Администрацию , в том числе в связи с предоставлением государственных и муниципальных услуг и исполнения муниципальных функций.

1.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения Администрации, сведения о лицах (за исключением сотрудников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Федеральный закон №152 - ФЗ);

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

- иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

1.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в случаях предусмотренных ч.8 ст. 14 Федерального закона № 152-ФЗ.

1.4. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.5. 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. Если субъект персональных данных считает, что Администрация осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152 - ФЗ или иным образом нарушает его права и свободу, субъект персональных данных вправе обжаловать действия или бездействие Администрации в уполномоченном органе по защите прав в субъектах персональных данных или в судебном порядке.

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

2. Порядок работы с запросами, уведомлениями и иными обращениями субъектов персональных данных или их представителей

2.1. При поступлении запроса, уведомления или иного обращения субъекта персональных данных или его представителя уполномоченными должностными лицами Администрации осуществляется его регистрация в журнале учета обращений субъектов персональных данных.

2.2. Уполномоченные должностные лица Администрации обязаны сообщить в порядке, предусмотренном ст. 14 Федерального закона № 152-ФЗ, субъекту персональных данных или его представителю информацию о наличии

персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

2.3. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или его персональных данных, субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя, уполномоченные должностные лица Администрации обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение п. 8 ст. 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

2.4. Уполномоченные должностные лица Администрации обязаны предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица Администрации обеспечивают внесение в них необходимых изменений. В срок, не превышающий 7 (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, уполномоченные должностные лица Администрации обязаны уничтожить такие персональные данные. Уполномоченные должностные лица Администрации обязаны уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

2.5. Уполномоченные должностные лица Администрации обязаны сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

2.6. Документальное оформление работы с запросами, уведомлениями и иными обращениями субъектов персональных данных и их представителей осуществляется в соответствии с примерными формами, приведенными в приложениях № 1 - 12 к настоящим Правилам.

2.7. Во всем ином, что не урегулировано настоящими Правилами, при работе с запросами, уведомлениями и иными обращениями по вопросам обработки персональных данных уполномоченные должностные лица Администрации руководствуются действующим законодательством.

Приложение № 1
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска»

В _____
(указать уполномоченный орган)

Уведомление об уничтожении
(примерная форма)

Настоящим уведомлением сообщаем вам, что в связи с _____
персональные данные _____уничтожены.
(указать персональные данные)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 2
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска»

В _____
(указать уполномоченный орган)

Уведомление об устранении допущенных нарушений
(примерная форма)

Настоящим уведомлением сообщаем вам, что допущенные нарушения при обработке персональных данных, а именно: _____
_____
(указать допущенные нарушения)
_____
_____ устранены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 3
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Запрос
(примерная форма)

Уважаемый(ая) _____ ,
(Ф.И.О.)

В связи с _____ у администрации города Южно-Сахалинска возникла необходимость получения следующей информации, составляющей Ваши персональные данные _____.
(перечислить информацию)

Просим Вас предоставить указанные сведения в течение _____ рабочих дней с момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение нами необходимой информации из следующих источников _____, следующими способами _____.

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения _____.

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 4
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска»

Уведомление о блокировании
(примерная форма)

Уважаемый(ая) _____ ,
(Ф.И.О.)
в связи с _____ сообщаем Вам, что Ваши персональные данные _____
(указать персональные данные)
заблокированы на срок _____.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 5
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Уведомление об уточнении
(примерная форма)

Уважаемый(ая) _____ ,
(Ф.И.О.)
в связи с _____ сообщаем Вам, что Ваши персональные данные уточнены в соответствии со сведениями: _____.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 6
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Уведомление
(примерная форма)

Уважаемый(ая) _____,
(Ф.И.О.)
администрацией города Южно-Сахалинска» производится обработка сведений, составляющих Ваши персональные данные:
_____.
(указать сведения)
Цели обработки: _____
_____.
Способы обработки: _____
_____.
Перечень лиц, которые имеют доступ к информации, содержащей Ваши персональные данные или могут получить такой доступ:

№ п.п.	Должность	Ф.И.О.	Вид доступа	Примечания

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения
_____
_____.
Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 7
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Уведомление об уничтожении
(примерная форма)

Уважаемый(ая) _____ ,
(Ф.И.О.)
в связи с _____ сообщаем Вам, что Ваши персональные данные _____уничтожены.
(указать персональные данные)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 8
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Уведомление об устранении допущенных нарушений
(примерная форма)

Уважаемый(ая) _____,
(Ф.И.О.)

в связи с _____ сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 9
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Мэру города Южно-Сахалинска
_____
от _____
(Ф.И.О., фактический
адрес проживания, тел.)

Заявление
(примерная форма)

Прошу заблокировать обрабатываемые Вами мои персональные данные:
_____
(указать блокируемые персональные данные)
на срок: _____;
(указать срок блокирования)
в связи с тем, что _____.
(указать причину блокирования персональных данных)

_____ _____
(подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 10
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Мэру города Южно-Сахалинска
_____
от _____
(Ф.И.О., фактический
адрес проживания, тел.)

Заявление
(примерная форма)

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки, предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ), сведения о том, какие юридические последствия для меня может повлечь ее обработка.

В случае отсутствия такой информации прошу Вас уведомить меня об этом.

_____ _____
(подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 11
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска

Мэру города Южно-Сахалинска
_____
от _____
(Ф.И.О., фактический
адрес проживания, тел.)

Заявление
(примерная форма)

Прошу уничтожить обрабатываемые Вами мои персональные данные: _____
(указать уничтожаемые персональные данные)
в связи с тем, что _____.
(указать причину уничтожения персональных данных)

_____ _____
(подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение № 12
к правилам рассмотрения запросов субъектов
персональных данных или их представителей
в администрации города Южно-Сахалинска»

Мэру города Южно-Сахалинска
_____
от _____
(Ф.И.О., фактический
адрес проживания, тел.)

Заявление
(примерная форма)

Прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями: _____
(указать уточненные персональные данные заявителя)
в связи с тем, что _____.
(указать причину уточнения персональных данных)

_____ _____
(подпись) (Ф.И.О.)

"___" _____ 20___ г.

Приложение №3

Утверждены
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными актами

1. Общие положения

1.1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города Южно-Сахалинска (далее - Администрация) организовывается проведение плановых и внеплановых проверок (далее — проверки) условий обработки персональных данных на предмет соответствия Федеральному закону от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Федеральный закон № 152-ФЗ) и постановлению Правительства Российской Федерации от 21.03.2012 № 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».

2. Тематика внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

2.1.1. Соответствие указанных в «Перечне персональных данных» персональных данных фактически обрабатываемым;

2.1.2. Актуальность Перечня должностей работников, замещение которых предусматривает осуществление обработки персональных данных;

2.1.3. Подтверждение факта ознакомления с локальными актами в

области обработки и обеспечения безопасности персональных данных;

2.1.4. Выборочные проверки уровня знания сотрудниками организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных;

2.1.5. Соблюдение пользователями информационных систем персональных данных (далее-ИСПДн) инструкции по учету, выдаче, хранению, обращению с машинными носителями информации и персональными идентификаторами, предназначенными для хранения информации ограниченного использования (персональными данными) (Приложение №3 к настоящим Правилам);

2.1.6. Соблюдение пользователями ИСПДн парольной политики;

2.1.7. Соблюдение пользователями ИСПДн антивирусной политики;

2.1.8. Соблюдение пользователями правил работы со средствами криптографической защиты информации (далее СКЗИ);

2.1.9. Соблюдение порядка доступа в помещения, где расположены элементы ИСПДн;

2.1.10. Соблюдение порядка работы со средствами защиты информации;

2.1.11. Знание пользователей ИСПДн о своих действиях во внештатных ситуациях;

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

2.2.1. Хранение бумажных носителей с персональными данными;

2.2.2. Доступ к бумажным носителям с персональными данными;

2.2.3. Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

3. Порядок проведения внутренних проверок

3.1. Проверки проводятся в соответствии с ежегодным Планом внутренних проверок условий обработки персональных данных Администрации (далее — План проверок) (примерная форма указана в Приложении №1 к настоящим Правилам) или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

3.2. Ежегодный План проверок разрабатывается комиссией по организации обработки и защиты персональных данных Администрации (далее — Комиссия) для осуществления внутреннего контроля соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом № 152 — ФЗ и утверждается председателем Комиссии.

3.3. Состав комиссии:

- председатель комиссии - первый вице-мэр, руководитель аппарата Администрации;

- заместитель председателя Комиссии - директор Департамента мобилизационной подготовки и защиты информации;

- члены комиссии :

- референт Департамента мобилизационной подготовки и защиты информации;

- руководитель проверяемого структурного подразделения аппарата или отраслевого (функционального) органа Администрации;

- администратор безопасности муниципальной информационной системы «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска».

3.4. В Плане проверок по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

3.5. Проверки проводятся Комиссией по организации обработки и защиты персональных данных. В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в ее результатах.

3.6. Основанием для проведения внеплановой проверки является поступившее в Администрацию письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

3.7. Проведение внеплановой проверки организуется в течение 5 рабочих дней с момента поступления обращения.

3.8. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.

3.9. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

3.10. По результатам каждой проверки Комиссией проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом (Приложение №2 к настоящим Правилам).

3.11. По существу поставленных в обращении (жалобе) вопросов Комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.

Приложение № 1
к правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

УТВЕРЖДАЮ
Первый вице-мэр,
руководитель аппарата Администрации
города Южно-Сахалинска
_____
"___" _____ 20__ г.

План
внутренних проверок условий обработки персональных данных
в администрации города Южно-Сахалинска
(примерная форма)

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие указанных в «Перечне персональных данных» персональных данных фактически обрабатываемым	Перечень персональных данных, обрабатываемых в администрации города Южно-Сахалинска»		
2.	Актуальность Перечня должностей работников, замещение которых предусматривает осуществление обработки персональных данных	Перечень должностей сотрудников администрации города Южно-Сахалинска, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным		
3.	Подтверждение факта ознакомления с локальными актами в области обработки и	Правила обработки персональных данных в администрации города Южно-Сахалинска		

	обеспечения безопасности персональных данных			
4.	Выборочные проверки уровня знания сотрудниками организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных	Правила обработки персональных данных в администрации города Южно-Сахалинска		
5.	Соблюдение пользователями ИСПДн инструкции по учету, выдаче, хранению, обращению с машинными носителями информации и персональными идентификаторами, предназначенными для хранения информации ограниченного использования	Инструкция по учету, выдаче, хранению, обращению с машинными носителями информации и персональными идентификаторами, предназначенными для хранения информации ограниченного использования		
6.	Соблюдение пользователями ИСПДн парольной политики	Правила обработки ПДн в администрации города Южно-Сахалинска, Положение о ЕМТС, Инструкция пользователю ЕМТС, Регламент использования ресурсов ЕМТС		
7.	Соблюдение пользователями ИСПДн антивирусной политики			
8.	Соблюдение пользователями правил работы со СКЗИ	Инструкция по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не		

		содержащей сведения, составляющие государственную тайну и криптоключами к ним		
9.	Соблюдение порядка доступа в помещения, где расположены элементы ИСПДн	Порядок доступа сотрудников администрации города Южно-Сахалинска в помещения, в которых ведется обработка ПДн		
10.	Соблюдение порядка работы со средствами защиты информации	Инструкция пользователю ЕМТС		
11.	Знание пользователей ИСПДн о своих действиях во внештатных ситуациях	Инструкция пользователя ЕМТС, Регламент использования ресурсов ЕМТС		
12.	Хранение бумажных носителей с персональными данными	Правила обработки ПДн в администрации города Южно-Сахалинска, Порядок доступа сотрудников администрации города Южно-Сахалинска в помещения, в которых ведется обработка ПДн		
13.	Доступ к бумажным носителям с персональными данными			
14.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными			

Заместитель Председателя комиссии _____ ФИО.

Приложение №2
к правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Протокол
проведения внутренней проверки условий обработки персональных данных в _____
(наименование подразделения)
администрации города Южно-Сахалинска

Настоящий Протокол составлен в том, что __.__. 20__ г. комиссией проведена проверка _____.
(тема проверки)

Проверка осуществлялась в соответствии с требованиями _____
_____

В ходе проверки проверено: _____
_____

Выявленные нарушения: _____
_____

Меры по устранению нарушений: _____
_____

Срок устранения нарушений: _____.

Председатель комиссии _____ФИО.

Заместитель председателя комисии _____ФИО

Члены:
Должность _____ ФИО.
Должность _____ ФИО.
Должность _____ ФИО.

Должность руководителя проверяемого подразделения администрации города Южно-Сахалинска» _____ ФИО.

Приложение №3
к правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Инструкция по учету, выдаче, хранению, обращению с машинными носителями информации и персональными идентификаторами, предназначенными для хранения информации ограниченного использования (персональными данными)

1. Общие положения

1.1. Все машинные носители информации, предназначенные для хранения информации ограниченного использования (для служебного использования, персональных данных) подлежат обязательному учету. Каждый съемный носитель с записанной на нем информацией ограниченного доступа должен иметь этикетку, на которой указывается его уникальный учетный номер.

1.2. Машинные носители информации учитываются в журнале учета. Журналы учета ведутся и хранятся в структурных подразделениях аппарата и отраслевых (функциональных) органах Администрации (далее — структурные подразделения), в которых ведется обработка информации ограниченного доступа.

1.3. Машинные носители информации выдаются и принимаются по журналу учета руководителем структурного подразделения.

1.4. Машинные носители информации в обязательном порядке маркируются следующим образом:

- на компакт-дисках (DVD, CD и др.) учетный номер проставляется на лицевой стороне диска специальным маркером;

- на жестком магнитном диске учетный номер проставляется на корпусе. Жесткий магнитный диск учитывается отдельно (в случае съемной конструкции) или в составе системного блока (СБ) автоматизированного рабочего места. В случае учета в составе СБ, на корпус СБ (в удобное для просмотра место) наклеивается бирка с указанием учетного номера, типа, модели машинного носителя, его объема, серийного номера жесткого магнитного диска;

- на носителях информации типа USB Flash-носители на корпус наклеивается бирка с указанием учетного номера носителя и его серийного номера;

- на персональных идентификаторах на корпус наклеивается бирка с указанием учетного номера носителя;

- бирки не должны закрывать заводские номера машинных носителей информации

1.5. Машинные носители информации хранятся в запертом шкафу.

1.6. Пользователям запрещается:

- использовать неучтенные машинные носители информации;

- использовать неучтенные персональные идентификаторы;

- хранить съемные носители с информацией ограниченного доступа вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с информацией ограниченного доступа из служебных помещений для работы с ними на дому.

1.7. При отправке или передаче информации ограниченного доступа адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка информации ограниченного доступа адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей информации ограниченного доступа для непосредственной передачи адресату осуществляется только с разрешения руководителя структурного подразделения.

1.8. О фактах утраты съемных носителей, содержащих информацию ограниченного доступа, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель структурного подразделения. На утраченные носители комиссией по организации обработки и защиты персональных данных составляется акт. Соответствующие отметки вносятся в Журнал учета магнитных, оптических и иных носителей информации.

1.9. Съемные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с информацией ограниченного доступа осуществляется комиссией по организации обработки и защиты персональных данных. По результатам уничтожения носителей информации составляется акт.

1.10. Сотрудники и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с информацией ограниченного доступа или персональным данным, должны быть в обязательном порядке ознакомлены под роспись с настоящей Инструкцией.

Приложение №4

Утверждены
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Правила
работы с обезличенными данными
в случае обезличивания персональных данных в
администрации города Южно-Сахалинска»

1. Общие положения

1.1. Настоящие Правила определяют порядок работы с обезличенными данными в случае обезличивания персональных данных в администрации города Южно-Сахалинска (далее — Администрация).

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.032012 № 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", постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказом Федеральной службы по техническому и экспертному контролю от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", приказом Роскомнадзора от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" (далее - приказ Роскомнадзора №996).

2. Порядок работы с обезличенными персональными данными

2.1. Обезличивание персональных данных в Администрации проводится с целью снижения ущерба от разглашения защищаемых персональных данных, снижения класса автоматизированных информационных систем, оператором которых является Администрация (далее - автоматизированные информационные системы) и по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей.

2.2. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

2.3. Обезличиванию подвергаются персональные данные, обработка которых осуществляется в автоматизированных информационных системах.

2.4. В процессе реализации процедуры обезличивания персональных данных следует соблюдать требования, предъявляемые к выбранному методу обезличивания, установленные приказом Роскомнадзора № 996.

2.5. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение парольной защиты средств автоматизации, идентификации пользователей в локальной сети, правил работы со съемными носителями (в случае их использования), правил резервного копирования, а также порядка доступа в помещения, где расположены информационные системы персональных данных, в целях исключения несанкционированного доступа к обезличенным персональным данным, а также исключения возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения, а также от неправомерных действий в отношении обезличенных персональных данных. Указанный порядок доступа обеспечивается в том числе:

- запиранием помещения на ключ, в том числе при выходе из помещения в рабочее время;

- закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие обезличенные персональные данные, во время отсутствия в помещении сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

2.6. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил хранения бумажных носителей и порядка доступа в помещения, где они хранятся, предусмотренного п. 2.5 настоящих Правил, в целях исключения несанкционированного доступа к обезличенным персональным данным, а также исключения возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения, а также от неправомерных действий в отношении обезличенных персональных данных.

Приложение №5

Утвержден
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Перечень
информационных систем персональных данных,
обрабатываемых в администрации города Южно-Сахалинска

Информационные системы персональных данных (далее - ИСПДн), обрабатываемых в администрации города Южно-Сахалинска включают :

- ИСПДн сотрудников администрации города Южно-Сахалинска;
- ИСПДн граждан, потребителей (абонентов) государственных и муниципальных услуг, исполнения муниципальных функций.

Приложение №6

Утвержден
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Перечень
персональных данных, обрабатываемых в администрации города Южно-Сахалинска в связи с реализацией трудовых отношений, а также в связи с оказанием государственных и муниципальных услуг и осуществлением государственных и муниципальных функций

№ п/п	Причина обработки персональных данных	Состав обрабатываемых персональных данных
1	Реализация трудовых отношений	фамилия, имя, отчество; пол; дата рождения; информация о смене фамилии, имени, отчества; дата рождения и место рождения; гражданство; документ, удостоверяющий личность (серия, номер, когда и кем выдан); заграничный паспорт; место рождения; место жительства и дата регистрации по месту жительства; информация о гражданстве; номера контактных телефонов; семейное положение; состав семьи (с указанием даты рождения, месте учебы (работы) ; отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах; сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, его серия и номер, дата выдачи); сведения об уровне специальных знаний (работа на

		компьютере, знание иностранного языка); сведения о профессиональной переподготовке, повышении квалификации, стажировке; ученая степень; сведения о трудовой деятельности, общем трудовом стаже и стаже государственной и/или муниципальной службы; сведения о замещаемой (занимаемой) должности; сведения о классных чинах, специальных званиях; сведения о состоянии здоровья и его соответствии выполняемой работе, наличии группы инвалидности и степени ограничения способности к трудовой деятельности; сведения об отпусках и командировках; сведения о прохождении аттестации; сведения о награждении (поощрении); сведения о взысканиях; сведения об отсутствии медицинских противопоказаний для прохождения муниципальной службы; сведения о пребывании за границей; сведения о судимости; сведения о допуске к государственной тайне; сведения о пенсионном обеспечении; сведения о трудовом договоре; реквизиты идентификационного номера налогоплательщика (ИНН); реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС); реквизиты полиса обязательного медицинского страхования; реквизиты свидетельства государственной регистрации актов гражданского состояния; сведения о доходах, имуществе и обязательствах имущественного характера и членов его семьи; (в случаях, установленных законодательством) сведения о социальных льготах; номера банковских счетов; фотография.
2	Предоставление государственных и муниципальных	фамилия, имя, отчество; документ, удостоверяющий личность (серия, номер, когда и кем выдан);

	услуг и исполнение государственных и муниципальных функций	дата рождения; место рождения; дееспособность; наличие группы инвалидности; наличие статуса ветеран ВОВ; наличие статуса многодетная семья; место жительства и дата регистрации по месту жительства; место работы; сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, его серия и номер, дата выдачи); номера контактных телефонов; сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка); сведения о профессиональной переподготовке, повышении квалификации, стажировке; реквизиты идентификационного номера налогоплательщика (ИНН); реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС); номера банковских счетов; сведения об имуществе; сведения о доходах; сведения о родственниках; сведения о судимости и реквизиты справки об освобождении; сведения о размере пенсии; сведения о состоянии здоровья.

Приложение №7

Утвержден
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Перечень
должностей в администрации города Южно-Сахалинска», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

1. Мэр города Южно-Сахалинска;
2. Первый вице-мэр;
3. Первый вице-мэр, руководитель аппарата;
4. Вице-мэр;
5. Руководители структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска.

Приложение №8

Утвержден
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Перечень
должностей в администрации города Южно-Сахалинска, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Должность	Основания для обработки	Способ обработки
1.	Мэр	Трудовой кодекс РФ, Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных, пункт № 1 Перечня Пдн.	Неавтоматизированный
2.	Первый вице-мэр	Трудовой кодекс РФ, Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных, пункт № 1 Перечня Пдн.	Неавтоматизированный
3.	Первый вице-мэр, руководитель аппарата	Трудовой кодекс РФ, Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных, пункт № 1 Перечня Пдн.	Неавтоматизированный
4.	Вице-мэр	Трудовой кодекс РФ, Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных, пункт № 1 Перечня Пдн.	Неавтоматизированный
5.	Директор Департамента социальной политики	Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», согласие субъекта персональных данных.	Автоматизированный

6.	Сотрудники Департамента социальной политики	Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», согласие субъекта персональных данных.	Автоматизированный
7.	Директор Департамента по обращениям граждан и организационной работе	Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
8.	Сотрудники Департамента по обращениям граждан и организационной работе	Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
9.	Директор Департамента кадровой политики	Трудовой Кодекс РФ, Федеральный закон от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации», Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
10.	Сотрудники Департамента кадровой политики	Трудовой Кодекс РФ, Федеральный закон от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации», Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
11.	Начальник Отдела по делам несовершеннолетних и защите их прав	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
12.	Сотрудники Отдела по делам несовершеннолетних и защите их прав	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный

13.	Директор Департамента образования	Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», согласие субъекта персональных данных.	Автоматизированный
14.	Сотрудники Департамента образования	Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», согласие субъекта персональных данных.	Автоматизированный
15.	Директор Правового департамента	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
16.	Сотрудники Правового департамента	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
17.	Директор Департамента внутренней политики	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
18.	Сотрудники Департамента внутренней политики	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
19.	Директор Департамента по делам молодежи, спорту и туризму	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
20.	Сотрудники Департамента по делам молодежи, спорту и туризму	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
21.	Директор Департамента общественной безопасности и контроля	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный

22.	Сотрудники Департамента общественной безопасности и контроля	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
23.	Директор Департамента землепользования	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
24.	Сотрудники Департамента землепользования	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
25.	Директор Департамента архитектуры и градостроительства	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
26.	Сотрудники Департамента архитектуры и градостроительства	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
27.	Директор Департамента по управлению муниципальным имуществом	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
28.	Сотрудники Департамента по управлению муниципальным имуществом	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
20.	Директор Департамента городского хозяйства	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный
30.	Сотрудники Департамента городского хозяйства	Устав городского округа «Город Южно-Сахалинск», согласие субъекта персональных данных.	Неавтоматизированный

Приложение №9

Утвержден
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Перечень
должностей в администрации города Южно-Сахалинска, доступ к персональным данным, которым необходим для выполнения служебных обязанностей

1. К персональным данным сотрудников администрации города Южно-Сахалинска, для выполнения своих должностных обязанностей имеют доступ:

- Мэр города Южно-Сахалинска;
- Первый вице-мэр;
- Первый вице-мэр, руководитель аппарата;
- Вице-мэр;
- Руководители и заместители руководителей департаментов, отделов администрации города Южно-Сахалинска;
- Все сотрудники Департамента кадровой политики;
- Сотрудники кадровых подразделений отраслевых (функциональных) органах администрации города Южно-Сахалинска.

2. К персональным данным граждан, обратившихся с жалобой, просьбой или на личном приеме, для выполнения своих должностных обязанностей имеют доступ:

- Мэр города Южно-Сахалинска;
- Первый вице-мэр;
- Первый вице-мэр, руководитель аппарата;
- Вице-мэр;
-Руководители и заместители руководителей структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска;
- Сотрудники соответствующих структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска.

3. К персональным данным граждан в связи с оказанием государственных и муниципальных услуг и осуществлением муниципальных функций для выполнения своих должностных обязанностей имеют доступ:

- Мэр города Южно-Сахалинска;
- Первый вице-мэр;

- Первый вице-мэр, руководитель аппарата;
- Вице-мэр;
- Руководители и заместители руководителей структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска;
- Сотрудники соответствующих структурных подразделений аппарата и отраслевых (функциональных) органов администрации города Южно-Сахалинска.

4. Каждый сотрудник Администрации имеет доступ к своим персональным данным.

5. Ответственность за работу с бумажными носителями персональных данных сотрудников администрации города южно-Сахалинска несут сотрудники Департамента кадровой политики.

6. Пользователи информационных систем персональных данных:

Перечень лиц, имеющих самостоятельный доступ к информационным ресурсам информационных систем персональных данных, уровень их полномочий и вид выполняемых функций определен в Положении о муниципальной информационной системы «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее — ЕМТС), Инструкции пользователя ЕМТС и Регламенте использования ресурсов ЕМТС.

Приложение №10

Утверждена
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Должностная инструкция
ответственного за организацию обработки персональных данных в администрации города Южно-Сахалинска

1. Общие положения

1.1. Должностная инструкция ответственного за организацию обработки персональных данных (далее - ПДн) в администрации города Южно-Сахалинска определяет основные обязанности и права ответственного за организацию обработки персональных данных.

1.2. Должностная инструкция регулирует отношения и порядок взаимодействия между ответственным за организацию обработки ПДн и сотрудниками, которые обрабатывают ПДн в связи с реализацией трудовых отношений, в связи с оказанием государственных и муниципальных услуг и осуществлением муниципальных функций, а также в соответствии с действующим законодательством Российской Федерации, за исключением случаев, перечисленных в части 2 статьи 1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в администрации города Южно-Сахалинска.

1.3. Деятельность ответственного лица за организацию обработки ПДн регламентируется федеральными законами и иными нормативными правовыми актами в области защиты персональных данных, актами Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, а также нормативно-правовыми актами администрации города Южно-Сахалинска.

2. Должностные обязанности

2.1 Организовывать работу по разработке и принятию организационно-распорядительной документации, устанавливать правила обработки ПДн, которые определяют:

- порядок доступа к ПДн;
- организацию приема и обработки обращений и запросов субъектов ПДн или их представителей;

- процедуры, направленные на предотвращение и выявление нарушений действующего законодательства Российской Федерации о персональных данных и устранения последствий таких нарушений;

2.2. Организовывать ознакомление сотрудников непосредственно осуществляющих обработку ПДн, с действующим законодательством Российской Федерации о персональных данных и организационно-распорядительной документации, определяющими правила обработки ПДн и требования по защите персональных данных.

2.3. Осуществлять согласование ввода в эксплуатацию новых информационных систем Пдн.

2.4. Координировать работу по формированию и ведению перечней:

- должностей сотрудников, замещение которых предусматривает осуществление обработки ПДн;
- персональных данных;
- информационных систем ПДн.

2.5. Организовывать проведение внутренних проверок по вопросам информационной безопасности для осуществления внутреннего контроля:

- условий обработки ПДн и их соответствие действующему законодательству Российской Федерации о ПДн и принятой в соответствии с ним организационно-распорядительной документацией;
- организации приема и обработки запросов субъектов ПДн или их представителей;
- выполнения установленных в соответствии с действующим законодательством Российской Федерации и организационно-распорядительной документацией требований к защите ПДн;
- соотношения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения действующего законодательства Российской Федерации о персональных данных и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством Российской Федерации и организационно-распорядительной документацией.

2.6. Представлять доклады директору Департамента мобилизационной работы и защиты информации о результатах проведенных внутренних проверок состояния работ по вопросам информационной безопасности и мерах, необходимых для устранения выявленных нарушений.

2.7. Координировать работу по принятию мер, направленных на совершенствование защиты ПДн.

2.8. Осуществлять методическое руководство работой при разработке условий обработки ПДн и эффективности мер по защите Пдн во вновь создаваемых ИСПДН.

3. Права

3.1. Ответственный за организацию обработки ПДн имеет право:

- запрашивать у сотрудников любые сведения, необходимые для организации условий обработки персональных данных и принятия необходимых правовых, организационных и технических мер для защиты ПДн;
- принимать участие в рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой ПДн, а также вырабатывать предложения для принятия в пределах своих полномочий решений по результатам рассмотрения указанных жалоб и обращений;
- участвовать в расследовании нарушений в области защиты ПДн и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;
- требовать от сотрудников уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн, при обращении (запросе) субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных либо по результатам проведенной внутренней проверки организации состояния работ по вопросам информационной безопасности;
- принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований действующего законодательства Российской Федерации о персональных данных;
- вносить предложения о совершенствовании нормативного правового регулирования обработки и защиты ПДн.

3.2. Докладывать директору Департамента мобилизационной подготовки и защиты информации о сотрудниках, имеющих санкционированный доступ к ПДн, допустивших серьезные нарушения в безопасности Пдн.

3.3. Требовать от сотрудников выполнения установленной технологии обработки Пдн, инструкций и других нормативных правовых документов по обеспечению безопасности Пдн.

3.4. Участвовать в разработке мероприятий по совершенствованию безопасности Пдн;

3.5. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых Пдн, технических средств из состава информационных систем, материальных носителей;

4. Ответственность

4.1. Ответственное лицо несет персональную ответственность за ненадлежащее выполнение возложенных на него обязанностей, изложенных в настоящей должностной инструкции, в соответствии с действующим

законодательством Российской Федерации и организационно-распорядительными документами.

4.2. Ответственное лицо несет персональную ответственность по действующему законодательству за разглашение конфиденциальной информации, ставшей известной ему по роду работы.

Ознакомлен:

Приложение №11

Утверждено
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Типовое обязательство сотрудника администрации города Южно-Сахалинска о неразглашении информации содержащей персональные данные на период исполнения им должностных обязанностей

Я, _____,
проживающий по адресу: _____
паспорт серия _____ № _____, выданный _____
(кем и когда)
предупрежден(а), что на период исполнения мною должностных обязанностей получаю доступ к персональным данным и во время исполнения своих обязанностей осуществляю их обработку (в том числе сбор, запись, систематизацию, накопление, хранение, уточнение, использование и передачу).

Я понимаю, что разглашение такого рода информации может нанести прямой и (или) косвенный ущерб субъектам персональных данных.

В связи с этим даю обязательство при обработке персональных данных строго соблюдать требования действующего законодательства, определяющего порядок обработки персональных данных, а также Правила обработки персональных данных в администрации города Южно-Сахалинска.

Я подтверждаю, что за исключением случаев и (или) при отсутствии условий, предусмотренных действующим законодательством, не имею права разглашать сведения, относящиеся к категории персональных данных.

Я предупрежден(а) о том, что в случае нарушения мною требований действующего законодательства и (или) Правил обработки персональных данных в администрации города Южно-Сахалинска, определяющих режим их обработки, в том числе в случае их незаконного разглашения или утраты, я несу ответственность в соответствии с действующим законодательством, в частности ст. 90 Трудового кодекса Российской Федерации.

С Правилами обработки персональных данных в администрации города Южно-Сахалинска ознакомлен(а).

_____ /_____/
подпись Фамилия

"___" _____ 20__ г.

Приложение №12

Утверждено
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Типовое обязательство сотрудника администрации города Южно-Сахалинска непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____,
проживающий по адресу: _____
паспорт серия _____ № _____, выданный _____
(кем и когда)
обязуюсь прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 г. №152-ФЗ "О персональных данных", я уведомлен(а) о том, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные, ставшие известными мне в связи с исполнением должностных обязанностей, без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных и о противодействии коррупции.

Положения законодательства Российской Федерации, предусматривающие ответственность за нарушение требований Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", мне разъяснены.

_____ /_____/
подпись Фамилия

"___" _____ 20__ г.

Приложение №13

Утверждена
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Типовая форма
согласия на обработку персональных данных сотрудника
администрации города Южно-Сахалинска,
иных субъектов персональных данных

Я, _____, проживающий(ая) по
(фамилия, имя, отчество)
адресу _____, основной документ, удостоверяющий личность (паспорт) _____
_____
(серия, номер, дата выдачи документа, наименование выдавшего органа)
даю свое согласие _____
(наименование (Ф.И.О.) и адрес оператора, получающего
_____
согласие субъекта персональных данных)
на обработку своих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, с целью _____.

Если мои персональные данные можно получить только у третьей стороны, то я должен(а) быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных. Для обработки указанных данных также должно быть получено мое согласие.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения моих персональных данных, а также мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Перечень персональных данных, на обработку которых дается согласие :

№ п.п	Персональные данные	Согласие	
		ДА	НЕТ
1. Общая информация			
	Фамилия		
	Имя		
	Отчество		
	Год, месяц, дата и место рождения		
	Адрес места жительства		
	Семейное положение		
	Социальное положение		
	Имущественное положение		
	Образование		
	Профессия		
	Доходы		
	(Другая информация)		
2. Специальные категории персональных данных			
	Состояние здоровья		
	(Другая информация)		
3. Биометрические данные			
	Дактилоскопическая информация		
	(Другая информация)		

Настоящее согласие действует _____
(срок).

Субъект персональных данных вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных в письменной форме (если иной порядок отзыва не предусмотрен действующим законодательством) оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

_____
(подпись субъекта персональных данных)

_____
(число, месяц, год)

Приложение №14

Утверждена
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Типовая форма
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
проживающий(ая) по адресу _____
_____,
(адрес места жительства субъекта персональных данных)
основной документ, удостоверяющий личность _____
_____
(наименование и номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе)
в соответствии с ч.2 ст. 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» настоящим подтверждаю, что мне разъяснены юридические последствия отказа предоставить свои персональные данные.

_____ _____
подпись Ф.И.О.

"___" _____ 20__ г.

Приложение №15

Утвержден
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Порядок
доступа сотрудников администрации города Южно-Сахалинска в помещения, в которых ведется обработка персональных данных

1. Общие положениями

1.1. Настоящий Порядок доступа сотрудников администрации города Южно-Сахалинска (далее - Администрация) в помещения, в которых ведется обработка персональных данных (далее - Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152 «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 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», и другими нормативными правовыми актами.

1.2. Ответственность за организацию и контроль доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей структурных подразделений аппарата и отраслевых (функциональных) органов Администрации.

1.3. Должностные лица Администрации, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.4. Помещения, в которых ведется обработка персональных данных, являются помещениями с ограниченным доступом.

1.5. Руководители структурных подразделений аппарата и отраслевых (функциональных) органов Администрации (далее - руководители подразделений) составляют и подписывают Перечень должностных лиц, имеющих право входа в помещение согласно Приложению к настоящему Порядку (далее – Перечень). Перечень вывешивается на внутренней стороне

двери помещения, в котором ведется обработка персональных данных. Перечень поддерживается в актуальном состоянии.

1.6. Сотрудники подразделений, на которых возложена обязанность по обработке персональных данных, несут персональную ответственность за выполнение мероприятий по предотвращению несанкционированного доступа к обрабатываемым персональным данным лицами (другими сотрудниками, работниками сторонних организаций, посетителями), которые не допущены к их обработке и ознакомлению.

2. Порядок доступа сотрудников, посетителей, работников контролирующих органов в помещения, в которых ведется обработка персональных данных

2.1. Доступ сотрудников подразделений в помещения, в которых ведется обработка персональных данных, осуществляется для выполнения ими своих служебных обязанностей и возложенных на них функций.

2.2. Доступ в конкретное помещение, в котором ведется обработка персональных данных, имеют только сотрудники, включенные в Перечень.

2.3. Сотрудники, посетители, работники сторонних организаций, прибывшие для решения служебных вопросов, ознакомления с документами, оформления и представления документов, допускаются в помещение, в котором ведется обработка персональных данных, с устного разрешения лиц, включенных в Перечень, и находятся в нем в их присутствии.

2.4. Сотрудники, прибывшие для проведения контрольных мероприятий, допускаются в помещение, в котором ведется обработка персональных данных, с устного разрешения руководителя подразделения.

2.5. Сотрудники контролирующих органов допускаются в помещение, в котором ведется обработка персональных данных при наличии соответствующего предписания на проведение контрольных мероприятий с разрешения мэра города Южно-Сахалинска (лица, его замещающего), в присутствии руководителя подразделения (лица, его замещающего).

2.6. Ознакомление с персональными данными лиц, прибывших для проведения контрольных мероприятий, осуществляется в объеме, предусмотренном планом проверки.

2.7. Сотрудники отвечающие за эксплуатацию средств вычислительной техники, прибывшие в помещение, в котором ведется обработка персональных данных, для выполнения своих должностных обязанностей, допускаются в помещение, в котором ведется обработка персональных данных, с разрешения руководителя подразделения (лица, его замещающего), в присутствии лиц, указанных в Перечне. Сотрудники отдела, указанные в Перечне, при проведении работ сотрудниками указанными выше обязаны принять меры по исключению ознакомления прибывших сотрудников с персональными

данными.

2.8. Сотрудники сторонних организаций, прибывшие в помещение, в котором ведется обработка персональных данных, для выполнения работ в соответствии с заключенным договором (контрактом), допускаются в помещение с разрешения руководителя подразделения (лица, его замещающего). При проведении таких работ, сотрудники, указанные в Перечне, обязаны принять меры по исключению ознакомления работников сторонних организаций с персональными данными.

3.Порядок сдачи и вскрытия помещений, в которых ведётся обработка персональных данных, под охрану

3.1. Сдачу (вскрытие) помещений, в которых ведется обработка персональных данных, под охрану осуществляют сотрудники подразделения, указанные в Перечне, или руководитель (лицо, его замещающее).

3.2.При сдаче помещения, в котором ведется обработка персональных данных, под охрану сотрудники обязаны выполнить следующие мероприятия:

- убрать документы с персональными данными в сейфы (запирающиеся шкафы) и опечатать их личной печатью;
- выключить установленным порядком компьютерную технику и оргтехнику;
- закрыть окна;
- выключить электроприборы;
- выключить свет;
- закрыть входную дверь на замок и опечатать дверь помещения личной печатью;
- сделать запись в Журнале приема и сдачи служебных помещений под охрану.

3.3. При вскрытии помещения, в котором ведется обработка персональных данных, сотрудники, вскрывающие помещение, обязаны выполнить следующие мероприятия:

- сделать запись в Журнале приема сдачи помещений под охрану;
- проверить целостность печати на входной двери помещения;
- вскрыть помещение;
- проверить целостность печатей на сейфах (шкафах), наличие и целостность компьютерной и оргтехники;
- при обнаружении нарушения целостности печатей, отсутствии или целостности компьютерной техники, других нарушениях прекратить вскрытие помещения, доложить о выявленных нарушениях своему руководителю и референту Департамента мобилизационной подготовки и защиты информации.

Приложение
к Порядку доступа сотрудников
администрации города
Южно-Сахалинска в помещения,
в которых ведется обработка
персональных данных

ПЕРЕЧЕНЬ

должностных лиц, имеющих право входа в помещение № ____
_____ администрации города Южно-Сахалинска

№	Должность	ФИО

Руководитель _____ _____

Примечание:

сотрудники, указанные в Перечне, допускаются в помещение для выполнения своих служебных обязанностей;

иные сотрудники, представители сторонних организаций при решении служебных вопросов допускаются в помещение с разрешения лиц, указанных в Перечне, и находятся в нем в их присутствии;

сотрудники, назначенные в состав комиссии по проведению контрольных мероприятий, допускаются в помещение на период проверки и находятся в помещении в присутствии лиц, указанных в Перечне;

сотрудники сторонних организаций, прибывшие для проведения контрольных мероприятий, допускаются в помещение после получения разрешения мэра города Южно-Сахалинск (лица, его замещающего), на период проверки и находятся в помещении в присутствии руководителя подразделения (лица, его замещающего);

сотрудники отвечающие за эксплуатацию средств вычислительной техники прибывшие в помещение для выполнения своих должностных обязанностей, допускаются в помещение с разрешения руководителя подразделения (лица, его замещающего), в присутствии лиц, указанных в Перечне;

работники сторонних организаций, прибывшие в помещение для выполнения работ в соответствии с заключенным договором (контрактом), допускаются в помещение с разрешения руководителя подразделения (лица, его замещающего) и находятся в помещении в присутствии лиц, указанных в Перечне.

Приложение №16

Утверждена
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Инструкция
по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и криптоключами к ним

1. Общие положения

1.1. Инструкция по порядку обращения с сертифицированными средствами криптографической защиты информации (далее - СКЗИ), предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее — Информация), и криптоключами к ним регламентирует порядок обращения с криптосредствами.

1.2. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами Российской Федерации:

- Состав и содержание 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 (утв. приказом ФСБ России от 10.07.2014 № 378);

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);

- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утв. приказом ФАПСИ от 13.06.2001 № 152).

1.3. Под криптосредством в настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации.

1.4. К криптосредствам (шифровальным, криптографическим средствам) относятся:

- средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

- средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

- средства электронной подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

- средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

- средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

- ключевые документы (независимо от вида носителя ключевой информации).

1.5. В настоящей Инструкции используются следующие понятия и определения:

- доступ к информации - возможность получения информации и ее использования;

- закрытый ключ - криптоключ, который хранится пользователем системы в тайне;

- ключевой документ - физический носитель определенной структуры, содержащий криптоключи;

- компрометация криптоключа - утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации;

- контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

- криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического

преобразования из числа всех возможных в данной криптографической системе;

- модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности;

- модель угроз - перечень возможных угроз;

- пользователь криптосредства - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования;

- средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.6. Для обеспечения безопасности Информации при ее обработке в информационных системах (далее - ИС) администрации города Южно-Сахалинска (далее - Администрация) должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.7. Класс криптосредства определяется в соответствии с Приказом Федеральной службы безопасности Российской Федерации 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».

2. Организационная структура

Безопасность обработки Информации в ИС Администрации с использованием криптосредств организует и обеспечивает ответственный за эксплуатацию СКЗИ в Администрации.

3. Обязанности пользователей криптосредств

3.1. Пользователи криптосредств допускаются к работе с ними только после получения заключения комиссии по организации обработки и защиты персональных данных о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и ознакомления под роспись с настоящей Инструкцией, другими документами, регламентирующими организацию и обеспечение безопасности Информации при ее обработке в ИС Администрации.

3.2. При наличии двух и более пользователей криптосредств обязанности

между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.3. Пользователи криптосредств обязаны:

- не нарушать конфиденциальность закрытых ключей;
- не допускать снятие копий с ключевых документов, содержащих закрытые ключи;
- не допускать вывод закрытых ключей на дисплей (монитор) автоматизированного рабочего места (далее - АРМ) или принтер;
- не допускать записи на ключевой документ посторонней информации;
- не допускать установки ключевых документов на другие АРМ;
- обеспечить конфиденциальность информации о криптосредствах, других мерах защиты;
- точно соблюдать требования к обеспечению безопасности Информации, требования к обеспечению безопасности криптосредств и ключевых документов к ним;
- хранить ключевые документы к криптосредствам в защищаемых хранилищах;
- сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей;
- своевременно выявлять и сообщать ответственному за эксплуатацию СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно уведомлять ответственного за эксплуатацию СКЗИ и принимать меры по предупреждению нарушения конфиденциальности Информации при утрате или недостаче криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности обрабатываемой Информации.

4. Учет ключевых документов

4.1. Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

4.2. Все экземпляры ключевых документов выдаются пользователям криптосредств под роспись в соответствующем журнале поэкземплярного учета.

4.3. Передача ключевых документов допускается только между пользователями криптосредств и ответственным за эксплуатацию СКЗИ под роспись в соответствующем Журнале поэкземплярного учета средств

криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями криптосредств осуществляется с письменного разрешения ответственного за эксплуатацию СКЗИ.

4.4. Для исключения компрометации ключевых документов на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища (ящики, шкафы) индивидуального пользования, которые в свою очередь закрываются на ключ и опечатываются.

4.5. Учет эксплуатационной и технической документации к криптосредствам:

- эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

4.6. Плановая смена ключевых документов:

- заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

4.7. Внеплановая смена ключевых документов:

- криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

4.8. Уничтожение ключевых документов:

- ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются ответственному за эксплуатацию СКЗИ или по его указанию уничтожаются на месте пользователями криптосредств;

- уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа;

- бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта;

- ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 (десяти) суток после вывода их из действия (окончания срока действия);

- пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом ответственного за эксплуатацию СКЗИ;

- уничтожение эксплуатационной и технической документации к

криптосредствам;

- эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

5. Техническое обслуживание криптосредств

5.1. Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.2. На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

6. Опечатывание аппаратных средств

Системные блоки АРМ, на которых установлены криптосредства, должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

7. Порядок доступа к хранилищам

Эксплуатация хранилищ:

- пользователи криптосредств хранят эксплуатационную и техническую документацию к криптосредствам, ключевые документы в хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;
- должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов;
- при необходимости доступа к содержимому хранилища сотрудник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа;
- по окончании работы сотрудник закрывает и опечатывает хранилище, за которое он ответственен;
- печати, предназначенные для опечатывания хранилищ, должны

находиться у сотрудников, ответственных за данные хранилища.

8. Контроль безопасности криптосредств

Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на ответственного за эксплуатацию СКЗИ в пределах его полномочий.

9. Ответственность за нарушение требований

9.1. Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

9.2. Ответственный за эксплуатацию СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки Информации с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Приложение №17
Утверждена
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Инструкция
ответственного за эксплуатацию средств
криптографической защиты информации

1. Общие положения

1.1. Настоящая Инструкция ответственного за эксплуатацию средств криптографической защиты информации (далее – СКЗИ) в Администрации города Южно-Сахалинска определяет основные обязанности и права ответственного за эксплуатацию СКЗИ.

1.2. Ответственный за эксплуатацию СКЗИ назначается постановлением Администрации города Южно-Сахалинска и отвечает за организацию, обеспечение функционирования и безопасность СКЗИ, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.3. Ответственный за эксплуатацию СКЗИ должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием СКЗИ.

1.4. В своей деятельности, связанной с обработкой персональных данных, ответственный за эксплуатацию СКЗИ руководствуется настоящей Инструкцией.

2. Обязанности ответственного за эксплуатацию СКЗИ

2.1. Вести поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним в соответствующем журнале.

2.2. Вести учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации в соответствующем журнале.

2.3. Осуществлять контроль за соблюдением условий использования криптосредств, установленных в эксплуатационной и технической документации на СКЗИ.

2.4. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах

защиты.

2.5. Соблюдать требования к обеспечению безопасности информации и требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.6. Сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним Директору департамента мобилизационной подготовки и защиты информации.

2.7. Немедленно уведомлять Директора департамента мобилизационной подготовки и защиты информации о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению информации ограниченного доступа.

2.8. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.9. Осуществлять ведение журнала поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов и журнала учёта хранилищ с ключевыми документами, а также ведение личных карточек (лицевых счетов) на каждого пользователя криптосредств.

3. Права ответственного за эксплуатацию СКЗИ

3.1. Инициировать разбирательство и составление заключений по фактам нарушения условий использования криптосредств, которые могут привести к нарушению безопасности информации или другим нарушениям, приводящим к снижению уровня защищенности.

3.2. Инициировать разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Приложение №18

Утверждена
постановлением администрации
города Южно-Сахалинска
от 21.02.2020 № 489-па

Политика
в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее — Политика) определяет принципы, порядок и условия обработки персональных данных сотрудников, соискателей и контрагентов администрации города Южно-Сахалинска и иных лиц, чьи персональные данные обрабатываются администрацией города Южно-Сахалинска, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Обеспечение конфиденциальности и безопасности обработки персональных данных в администрации города Южно-Сахалинска является одной из приоритетных задач.

1.3. В администрации города Южно-Сахалинска для этих целей введен в действие комплект организационно-распорядительной документации, обязательный к исполнению всеми сотрудниками администрации города Южно-Сахалинска, допущенными к обработке персональных данных.

1.4. Обработка, хранение и обеспечение конфиденциальности и безопасности персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации в сфере защиты персональных данных, и в соответствии с муниципальными правовыми актами администрации города Южно-Сахалинска.

1.5. В настоящей Политике используются понятия, установленные в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных (далее-Федеральный закон №152-ФЗ).

1.6. Администрация города Южно-Сахалинска является оператором, организующим и осуществляющим обработку персональных данных, а так же

определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2. Понятие и состав персональных данных

2.1. Сведениями, составляющими персональные данные, в администрации города Южно-Сахалинска является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. Перечень персональных данных, подлежащих защите в администрации города Южно-Сахалинска определятся целями их обработки, Федеральным законом № 152-ФЗ, Трудовым кодексом РФ и другими нормативно-правовыми актами.

2.3. В администрации города Южно-Сахалинска утвержден перечень персональных данных подлежащих защите.

2.4. В администрации города Южно-Сахалинска обрабатываются следующие персональные данные сотрудников: фамилия, имя, отчество, пол, дата рождения, информация о смене фамилии, имени, отчества, дата рождения и место рождения; гражданство, документ, удостоверяющий личность (серия, номер, когда и кем выдан), заграничный паспорт, место рождения, место жительства и дата регистрации по месту жительства, информация о гражданстве, номера контактных телефонов, семейное положение, состав семьи (с указанием даты рождения, месте учебы (работы), отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах, сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, его серия и номер, дата выдачи), сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка),сведения о профессиональной переподготовке, повышении квалификации, стажировке, ученая степень, сведения о трудовой деятельности, общем трудовом стаже и стаже государственной и/или муниципальной службы; сведения о замещаемой (занимаемой) должности; сведения о классных чинах, специальных званиях; сведения о состоянии здоровья и его соответствии выполняемой работе, наличии группы инвалидности и степени ограничения способности к трудовой деятельности; сведения об отпусках и командировках, сведения о прохождении аттестации, сведения о награждении (поощрении), сведения о взысканиях, сведения об отсутствии медицинских противопоказаний для прохождения муниципальной службы, сведения о пребывании за границей, сведения о судимости, сведения о допуске к государственной тайне, сведения о

пенсионном обеспечении, сведения о трудовом договоре, реквизиты идентификационного номера налогоплательщика (ИНН), реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС), реквизиты полиса обязательного медицинского страхования, реквизиты свидетельства государственной регистрации актов гражданского состояния, сведения о доходах, имуществе и обязательствах имущественного характера и членов его семьи (в случаях, установленных законодательством) сведения о социальных льготах; номера банковских счетов, фотография.

2.5. В администрации города Южно-Сахалинска обрабатываются следующие персональные данные в связи с предоставлением государственных и муниципальных услуг и исполнение муниципальных функций: фамилия, имя, отчество, документ, удостоверяющий личность (серия, номер, когда и кем выдан), дата рождения, место рождения, дееспособность, наличие группы инвалидности, наличие статуса ветеран ВОВ, наличие статуса многодетная семья, место жительства и дата регистрации по месту жительства, место работы, сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, его серия и номер, дата выдачи), номера контактных телефонов, сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка), сведения о профессиональной переподготовке, повышении квалификации, стажировке, реквизиты идентификационного номера налогоплательщика (ИНН), реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС), номера банковских счетов, сведения об имуществе, сведения о доходах, сведения о родственниках, сведения о судимости и реквизиты справки об освобождении, сведения о размере пенсии, сведения о состоянии здоровья.

3. Цели сбора персональных данных

Администрация города Южно-Сахалинска осуществляет обработку персональных данных в следующих целях:

- организация кадрового учета, обеспечение соблюдения законов и иных нормативно-правовых актов, ведение кадрового делопроизводства, исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации;

- подбор кандидатов на вакантные должности;
- предоставление государственных и муниципальных услуг и исполнение муниципальных функций.

4. Правовые основания обработки персональных данных

Персональные данные в администрации города Южно-Сахалинска обрабатываются на основании:

- Трудового кодекса Российской Федерации;
- Федерального закона №152-ФЗ ;
- Федерального закона от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Федерального закона от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации»;
- договоров, заключаемых между администрацией города Южно-Сахалинска и субъектом персональных данных;
- согласия на обработку персональных данных.

5. Сроки обработки персональных данных

5.1. Сроки обработки персональных данных определяются в соответствии со сроком действия договора (соглашением) с субъектом персональных данных, Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», сроком исковой давности, а также иными требованиями законодательства РФ.

5.2. В администрации города Южно-Сахалинска создаются и хранятся документы, содержащие сведения о субъектах персональных данных.

5.3. Требования к использованию в администрации города Южно-Сахалинска данных типовых форм документов установлены постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Права и обязанности

6.1. Администрация города Южно-Сахалинска как оператор персональных данных в праве:

- отстаивать свои интересы в суде;

- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

- отказывать в предоставлении персональных данных в случаях предусмотренных федеральным законодательством;

- использовать персональные данные субъекта без его согласия, в случаях предусмотренных федеральным законодательством.

6.2. Администрация города Южно-Сахалинска, как оператор персональных данных обязана:

- обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, содержащими его персональные данные, если иное не предусмотрено федеральным законом;

- внести необходимые изменения, уничтожить или блокировать персональные данные в случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных, а также уведомить о своих действиях субъекта персональных данных;

- выполнять иные обязанности оператора, предусмотренные Федеральным законом №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

6.3. Субъект персональных данных имеет право:

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

- требовать перечень своих персональных данных, обрабатываемых администрацией города Южно-Сахалинска и источник их получения;

- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

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

- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

- на получение информации, касающейся обработки его персональных данных, в том числе содержащей иные сведения, предусмотренные Федеральным законом №152-ФЗ и другими федеральными законами.

7. Порядок и условия обработки персональных данных

7.1. Администрация города Южно-Сахалинска осуществляет как

автоматизированную, так и неавтоматизированную обработку персональных данных.

7.2. Под обработкой персональных данных в администрации города Южно-Сахалинска понимается сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.3. Персональные данные не передаются третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

7.4 Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

7.5. Обработка персональных данных в администрации города Южно-Сахалинска производится на основе соблюдения принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

7.6. Отказ контрагента или сотрудника администрации города Южно-Сахалинска от предоставления согласия на обработку его персональных данных влечет за собой невозможность достижения целей обработки.

8. Обеспечение безопасности персональных данных

8.1. Администрация города Южно-Сахалинска предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

8.2. Администрация города Южно-Сахалинска для обеспечения безопасности персональных данных осуществляет следующие меры:

- назначение лица, ответственного за организацию обработки персональных данных;

- назначение администратора безопасности информационной системы персональных данных;

- принятие документов, определяющих политику администрации города Южно-Сахалинска в отношении обработки персональных данных и устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- осуществление внутреннего контроля соответствия обработки персональных данных законодательству Российской Федерации в данной сфере;

- разработка модели угроз безопасности, в которой при определении опасности угроз проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона №152-ФЗ;

- для информационной системы персональных данных разработка технического задания на создание системы защиты информации;

- проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;

- ознакомление сотрудников, допущенных к обработке персональных данных с положениями законодательства Российской Федерации о персональных данных и документами определяющими политику администрации города Южно-Сахалинска в отношении обработки персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

9. Заключительные положения

9.1. К настоящей Политике обеспечивается неограниченный доступ.

9.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

9.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных в администрации города Южно-Сахалинска.

9.4. Ответственность должностных лиц администрации города Южно-

Сахалинска, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами администрации города Южно-Сахалинска.