**АДМИНИСТРАЦИЯ**

**ПУГАЧЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**САРАТОВСКОЙ ОБЛАСТИ**

**РАСПОРЯЖЕНИЕ**

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Об утверждении Положения о порядке обработки и обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации Пугачевского муниципального района**

В целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, руководствуясь Федеральным Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»:

1. Утвердить Положение о порядке обработки и обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации Пугачевского муниципального района согласно приложению.

2. Ответственному за организацию и контроль мероприятий по защите персональных данных в администрации Пугачевского муниципального района (М.В. Орловскому) ознакомить служащих администрации Пугачевского муниципального района, непосредственно осуществляющих обработку персональных данных, с положениями настоящего распоряжения.

3. Отделу информации, анализа и общественных отношений (Грибанова Т.Ю.) разместить распоряжение на официальном сайте администрации Пугачевского муниципального района.

4. Контроль за исполнением распоряжения возложить на управляющего делами администрации Пугачевского муниципального района Бабухина Н.В.

**Глава администрации Пугачевского**

**муниципального района С.А. Сидоров**

Приложение к распоряжению администрации Пугачевского муниципального района

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_\_

**ПОЛОЖЕНИЕ**

**о порядке обработки и обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации Пугачевского муниципального района**

1. Общие положения

1. **Правовые и нормативно-методические источники документа**

Настоящее Положение о порядке обработки и обеспечения безопасности персональных данных в информационных системах персональных данных администрации Пугачевского муниципального района разработано в соответствии со следующими нормативно-правовыми документами:

* Федеральный закон Российской Федерации от 27 июля 2006г. №152-ФЗ «О персональных данных»;
* Федеральный закон Российской Федерации от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Постановление Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* Постановление Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 18 февраля 2013г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
* методические документы ФСБ России, ФСТЭК России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.
1. **Термины и определения:**

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Документированная информация** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

**Заявитель** - физическое или юридическое лицо (за исключением государственных органов и их территориальных органов, органов государственных внебюджетных фондов и их территориальных органов, органов местного самоуправления) либо их уполномоченные представители, обратившиеся в орган исполнительной власти с запросом о предоставлении государственной или муниципальной услуги, выраженным в устной, письменной или электронной форме.

**Информационная система персональных данных** (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**Конфиденциальная информация** — информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

**Конфиденциальность персональных данных** – операторы и иные лица, получившие доступ к персональным данным, если иное не предусмотрено федеральным законом, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

**Обработка персональных данных** - любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

**Персональная ответственность** – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Система защиты персональных данных** - комплекс организационных мер и программно-технических средств защиты информации от несанкционированного доступа к информации в информационной системе персональных данных;

**Трансграничная передача персональных данных -** передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1. **Назначение положения**

Целью документа является определение порядка получения, использования, обработки, хранения, доступа, передачи персональных данных субъектов ПД; обеспечение защиты прав и свобод субъектов ПД при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным субъектов, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1. **Область действия документа**

Настоящий документ предназначен для пользователей информационных систем персональных данных администрации Пугачевского муниципального района, которые в рамках своих должностных обязанностей имеют доступ и (или) осуществляют обработку персональных данных субъектов ПД.

1. **Цели обработки персональных данных**

Целью обработки персональных данных является обработка персональных данных сотрудников администрации Пугачевского муниципального района в рамках трудового законодательства, а также предоставление структурными подразделениями администрации Пугачевского муниципального района государственных и муниципальных услуг субъектам персональных данных.

# 2. Общие требования при обработке ПД

В целях обеспечения прав и свобод человека и гражданина при обработке ПД обязаны соблюдаться следующие требования:

персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации;

обработка персональных данных ограничивается достижением заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных;

содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

при принятии решений, затрагивающих интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения;

пользователи информационных систем персональных данных администрации Пугачевского муниципального района должны быть ознакомлены под роспись с документами администрации Пугачевского муниципального района, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области;

физические и юридические лица – субъекты ПД или их законные представители имеют право ознакомиться с документами администрации Пугачевского муниципального района (оператора), устанавливающими порядок обработки их персональных данных, а также их права и обязанности в этой области.

субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

#

# 3. Основные условия проведения обработки персональных данных

Обработка персональных данных осуществляется:

1. после получения согласия субъекта персональных данных, за исключением случаев, если:

а) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

б) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

в) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

г) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

д) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

е) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

ж) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

з) обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

и) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

к) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1. после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Саратовской области, за исключением случаев, если персональные данные:

а) обрабатываются в соответствии с трудовым законодательством;

б) получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

в) относятся к членам (участникам) общественного объединения или религиозной организации и обрабатываются соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

г) сделаны субъектом персональных данных общедоступными;

д) включают в себя только фамилии, имена и отчества субъектов персональных данных;

е) необходимы в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

ж) включены в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

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

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

1. после принятия необходимых мер по защите персональных данных.

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

Распоряжением администрации Пугачевского муниципального района назначается Администратор информационной безопасности (ИБ), и определяется перечень сотрудников, допущенных к обработке персональных данных в информационных системах персональных данных администрации Пугачевского муниципального района.

Запрещается:

1. обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
2. осуществлять ввод персональных данных под диктовку.

# 4. Обработка персональных данных с использованием средств автоматизации

Автоматизированная обработка персональных данных в информационных системах персональных данных администрации Пугачевского муниципального района ведется:

с использованием технических средств, удовлетворяющих уровню защищенности персональных данных в информационных системах персональных данных администрации Пугачевского муниципального района;

 при утвержденной организационно-распорядительной документации.

Не допускается обработка персональных данных в информационных системах персональных данных администрации Пугачевского муниципального района если не обеспечена конфиденциальность и требования по защите указанных данных.

При автоматизированной обработке различных категорий персональных данных должен использоваться отдельный электронный носитель информации для каждой категории персональных данных.

При отсутствии технологической возможности осуществления автоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению № 1.

Учет электронных носителей информации, содержащих персональные данные, осуществляется администратором информационной безопасности администрации Пугачевского муниципального района.

При несовместимости целей автоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

 при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

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

# 5. Получение персональных данных

При поступлении на муниципальную службу гражданин предоставляет:

заявление с просьбой о поступлении на муниципальную службу и замещении должности муниципальной службы;

собственноручно заполненную и подписанную анкету по форме, установленной уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти;

паспорт;

трудовую книжку, за исключением случаев, когда трудовой договор (контракт) заключается впервые;

документ об образовании;

страховое свидетельство обязательного пенсионного страхования, за исключением случаев, когда трудовой договор (контракт) заключается впервые;

свидетельство о постановке физического лица на учет в налоговом органе по месту жительства на территории Российской Федерации;

документы воинского учета - для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу;

заключение медицинской организации об отсутствии заболевания, препятствующего поступлению на муниципальную службу;

сведения о доходах за год, предшествующий году поступления на муниципальную службу, об имуществе и обязательствах имущественного характера;

иные документы, предусмотренные федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

В целях предоставления государственных или муниципальных услуг в электронной форме основанием для начала предоставления государственной или муниципальной услуги является направление заявителем с использованием единого портала государственных и муниципальных услуг сведений из следующих документов:

документы, удостоверяющие личность гражданина Российской Федерации, в том числе военнослужащих, а также документы, удостоверяющие личность иностранного гражданина, лица без гражданства, включая вид на жительство и удостоверение беженца;

документы воинского учета;

свидетельства о государственной регистрации актов гражданского состояния;

документы, подтверждающие регистрацию по месту жительства или по месту пребывания;

документы, подтверждающие предоставление лицу специального права на управление транспортным средством соответствующего вида;

документы, подтверждающие прохождение государственного технического осмотра (освидетельствования) транспортного средства соответствующего вида;

документы на транспортное средство и его составные части, в том числе регистрационные документы;

документы о трудовой деятельности, трудовом стаже и заработке гражданина;

документы о соответствующих образовании и (или) профессиональной квалификации, об ученых степенях и ученых званиях и документы, связанные с прохождением обучения, выдаваемые организациями, осуществляющими образовательную деятельность;

справки, заключения и иные документы, выдаваемые медицинскими организациями, осуществляющими медицинскую деятельность и входящими в государственную, муниципальную или частную систему здравоохранения;

документы Архивного фонда Российской Федерации и другие архивные документы в соответствии с законодательством об архивном деле в Российской Федерации, переданные на постоянное хранение в государственные или муниципальные архивы;

решения, приговоры, определения и постановления судов общей юрисдикции и арбитражных судов;

учредительные документы юридического лица;

решения, заключения и разрешения, выдаваемые органами опеки и попечительства в соответствии с законодательством Российской Федерации об опеке и попечительстве;

правоустанавливающие документы на объекты недвижимости, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

документы, выдаваемые федеральными государственными учреждениями медико-социальной экспертизы;

удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки;

документы о государственных и ведомственных наградах, государственных премиях и знаках отличия

если иное не предусмотрено законодательными актами при регламентации предоставления государственной или муниципальной услуги.

Запрещается получать и иным способом обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности политических, религиозных, философских и иных убеждениях, состояния здоровья, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

#

# 6. Передача персональных данных

Предоставление персональных данных субъекта производится в соответствии с требованиями действующего законодательства Российской Федерации.

При передаче персональных данных заявителя оператор обязан соблюдать следующие требования:

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

предоставление персональных данных субъекта уполномоченному органу по защите прав субъектов ПД, на который возлагаются функции обеспечения контроля и надзора за соответствием обработки ПД требованиям ФЗ №-152, осуществляется по запросу (указанный уполномоченный орган имеет право запрашивать у органов исполнительной власти информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию).

в случае если лицо, обратившееся к администрации Пугачевского муниципального района с запросом на предоставление персональных данных, не уполномочено на получение информации, относящейся к персональным данным, администрация Пугачевского муниципального района обязана отказать лицу в выдаче такой информации. Лицу, обратившемуся с соответствующим запросом, выдается уведомление в свободной форме об отказе в выдаче информации, а копия уведомления хранится в соответствии с принятыми правилами делопроизводства (как исходящая корреспонденция).

# 7. Доступ к персональным данным

* 1. **Организация допуска к ПД**

Доступ к персональным данным субъектов персональных данных имеют только сотрудники, являющиеся пользователями информационных систем персональных данных администрации Пугачевского муниципального района.

Доступ к персональным данным субъектов других работников администрации Пугачевского муниципального района, не имеющих надлежащим образом оформленного допуска, запрещается.

### Доступ к ПД

Администрация Пугачевского муниципального района не допускает распространение ПД без согласия субъекта ПД или наличия иного законного основания, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных.

Лица, имеющие доступ к персональным данным субъектов ПД, обязаны соблюдать требования по нераспространению персональных данных.

Сотрудники администрации Пугачевского муниципального района, являющиеся пользователями информационных систем персональных данных администрации Пугачевского муниципального района, должны быть ознакомлены под роспись с настоящим документом, с иными документами, устанавливающими порядок обработки персональных данных субъектов ПД в информационных системах персональных данных администрации Пугачевского муниципального района, а также об их правах и обязанностях в этой области.

Субъект ПД имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные, за исключением случаев, когда:

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

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

обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

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

Субъект имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

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

 подтверждение факта обработки персональных данных администрацией Пугачевского муниципального района, а также правовые основания и цель такой обработки;

 способы обработки персональных данных, применяемые администрацией Пугачевского муниципального района;

 сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

 перечень обрабатываемых персональных данных и источник их получения;

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

 порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

 иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими федеральными законами.

Доступ к своим персональным данным предоставляется субъекту ПД или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

# 8. Контроль защиты персональных данных. Порядок разбирательства по фактам нарушения требований по защите персональных данных и принятие мер по предотвращению возможных опасных последствий

Ведение контроля защиты персональных данных осуществляется путем проведения периодических, плановых и внеплановых проверок объектов защиты. Периодические, плановые и внеплановые проверки объектов защиты проводятся, как правило, силами администратора информационной безопасности (ИБ) информационных систем персональных данных администрации Пугачевского муниципального района и(или) ответственного за обеспечение безопасности ПД администрации Пугачевского муниципального района,в соответствии с утвержденным планом или по согласованию с главой администрации Пугачевского муниципального района.

При обнаружении нарушений требований по защите ПД администратор ИБ докладывает о нарушении главе администрации Пугачевского муниципального района. Глава администрации Пугачевского муниципального района должен принять решение о продолжении или прекращении обработки ПД и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля системы защиты ПД оформляются администратором ИБ в виде актов.

Невыполнение предписанных мероприятий по защите ПД, считается предпосылкой к утечке ПД (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию главы администрации Пугачевского муниципального района или ответственного за обеспечение безопасности ПД администрации Пугачевского муниципального района проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора ИБ. Комиссия должна установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие. Так же комиссия устанавливает лиц, виновных в нарушении предписанных мероприятий по защите персональных данных, выясняет причины и условия, приводящие к нарушению, и вырабатывает рекомендации по их устранению. После окончания расследования глава администрации Пугачевского муниципального района принимает решение о мерах, применяемых к виновным лицам, и необходимых мероприятиях по устранению недостатков.

Мероприятия по физическому контролю доступа включают:

 мероприятия по контролю доступа на территорию;

 мероприятия по контролю доступа в помещения с оборудованием ИСПДн;

 мероприятия по контролю доступа к техническим средствам ИСПДн;

 мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории администрации Пугачевского муниципального района.

Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными замками или приспособлениями для опечатывания. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются автоматизированные рабочие места (АРМ) пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки персональных данных (обслуживающий персонал, другие сотрудники), должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не допущенных к обработке персональных данных.

При выносе устройств, хранящих персональные данные, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации хранимой на этих устройствах.

# 9. Реагирование на нештатные ситуации

При возникновении инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями затрагивающими безопасность персональных данных, проводится соответствующее расследование нештатных ситуаций.

В рамках расследования решаются следующие задачи:

 расследование инцидентов, связанных с безопасностью персональных данных;

 ликвидация последствий инцидентов связанных с безопасностью персональных данных;

 принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

# 10. Блокирование персональных данных

В случае выявления недостоверных персональных данных субъекта ПД или неправомерных действий с ними пользователей информационных систем персональных данных администрации Пугачевского муниципального района, при обращении или по запросу субъекта ПД или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных осуществляется блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки.

В случае подтверждения факта недостоверности персональных данных субъекта ПД на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов производится уточнение персональных данных, соответствующая блокировка снимается.

В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с момента выявления, необходимо устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий десяти рабочих дней с момента выявления неправомерности действий с персональными данными, необходимо уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных администрация Пугачевского муниципального района обязана уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

# 11. Резервирование персональных данных

Резервирование персональных данных должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на различные носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

# 12. Права и обязанности субъектов ПД и оператора

Субъект ПД имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев, предусмотренных п.8 ст.14 Федерального закона №152-ФЗ «О персональных данных»), содержащей его персональные данные. Субъект имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

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

 подтверждение факта обработки персональных данных администрацией Пугачевского муниципального района, а также правовые основания и цель такой обработки;

 способы обработки персональных данных, применяемые администрацией Пугачевского муниципального района;

 сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

 перечень обрабатываемых персональных данных и источник их получения;

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

 порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;

иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими федеральными законами.

Субъект персональных данных может обжаловать действия или бездействие администрации Пугачевского муниципального района в установленном законом порядке, если субъект персональных данных, считает, что обработка его персональных данных осуществляется с нарушением требований Федерального закона № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы.

Права и обязанности Оператора:

 оператор обязан принимать необходимые и достаточные меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

 оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

# 13. Организация системы защиты персональных данных в администрации Пугачевского муниципального района

Система защиты персональных данных является частью общей системы обеспечения информационной безопасности администрации Пугачевского муниципального района.

Основой системы защиты персональных данных являются:

руководитель;

ответственный за обеспечение безопасности персональных данных;

администратор безопасности ИСПДн;

ответственные за техническое сопровождение ИСПДн;

структурные подразделения, участвующие в процессах обработки персональных данных;

сотрудники администрации Пугачевского муниципального района.

Руководитель в рамках своих полномочий осуществляет следующие функции в области обеспечения безопасности персональных данных:

 обеспечивает общую организацию работ по защите персональных данных;

 утверждает нормативные документы по вопросам организации системы защиты персональных данных, а также документы, регламентирующие обработку и защиту персональных данных

 назначает ответственных за обеспечение безопасности персональных данных;

 заслушивает при необходимости ответственных за обеспечение безопасности персональных данных и других должностных лиц о состоянии работ по защите персональных данных.

Ответственный за обеспечение безопасности персональных данных осуществляют следующие основные функции:

 разрабатывает Перечень персональных данных, подлежащих защите в администрации Пугачевского муниципального района;

 участвует в проведении определении уровня защищенности ИСПДн;

 распределяет ответственность по вопросам обработки и защиты персональных данных;

 определяет допустимые сроки хранения персональных данных по каждой категории персональных данных;

 организует подачу уведомлений в уполномоченный орган по защите прав субъектов персональных данных;

 заслушивает руководителей структурных подразделений, участвующих в обработке персональных данных и построении системы защиты персональных данных, о принимаемых мерах по состоянию и совершенствованию системы защиты персональных данных;

 организует работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты персональных данных;

 осуществляет организацию плановых и внеплановых проверочных мероприятий;

 организует выполнение требований по защите персональных данных в администрации Пугачевского муниципального района;

 проводит разработку и актуализацию локальных нормативных документов, регламентирующих защиту персональных данных в администрации Пугачевского муниципального района;

 проводит ознакомление сотрудников с нормативными документами в области защиты персональных данных;

 проводит оценку эффективности принятых мер и применяемых средств защиты персональных данных;

 проводит занятия с сотрудниками администрации Пугачевского муниципального района по изучению организационно-распорядительных документов по всему комплексу вопросов защиты персональных данных;

 разрабатывает и актуализирует частные модели угроз безопасности персональных данных и технические задания на систему защиты персональных данных;

 определяет необходимость обучения сотрудников по вопросам обеспечения безопасности персональных данных;

 контролирует выполнение сотрудниками требований по защите персональных данных;

 организует работы по сбору сведений об изменениях в составе и структуре ИСПДн;

 осуществляет контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов по защите персональных данных, а также внутренних организационно-распорядительных документов администрации Пугачевского муниципального района;

 контролирует исполнение требований по уничтожению персональных данных;

 разрабатывает рекомендации по оптимизации существующих и новых информационных процессов обработки персональных данных по критериям соответствия требованиям по защите персональных данных и минимизации затрат на создание и эксплуатацию системы защиты персональных данных;

 контролирует исполнение требований нормативных документов оператора в области обеспечения безопасности персональных данных, структурными подразделениями и сотрудниками администрации Пугачевского муниципального района;

 организует и осуществляет взаимодействие с регуляторами по вопросам защиты персональных данных;

 участвует в аттестации (декларировании соответствия) ИСПДн администрации Пугачевского муниципального района по требованиям безопасности информации;

 управляет проектами по внедрению систем и средств защиты персональных данных;

 контролирует ввод в действие, эксплуатацию системы защиты персональных данных;

 участвует в расследовании инцидентов, связанных с нарушением безопасности персональных данных, правил обработки персональных данных, принимает меры по недопущению повторения нештатных ситуаций.

Администратор безопасности ИСПДн осуществляет следующие функции:

 осуществляет сопровождение средств и систем защиты персональных данных;

 проводит оперативный контроль функционирования средств и систем защиты персональных данных;

 проводит резервирование персональных данных;

 ведет учет носителей персональных данных;

 осуществляет выявление и регистрацию попыток несанкционированного доступа к компонентам ИСПДн, информационным ресурсам;

 контролирует соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и системой защиты персональных данных;

 осуществляет учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

 контролирует выполнение сотрудниками администрации Пугачевского муниципального района требований по защите персональных данных;

 участвует в расследованиях причин возникновения нештатных ситуаций;

 осуществляет подготовку предложений по совершенствованию системы защиты персональных данных в администрации Пугачевского муниципального района;

 выполняет комплекс мероприятий по защите информации при проведении ремонтных и регламентных работ;

 обеспечивают защиту персональных данных при выводе из эксплуатации компонентов ИСПДн.

Ответственные за техническое сопровождение ИСПДн осуществляют следующие функции:

 осуществляют сопровождение технических средств и систем ИСПДн.

Структурные подразделения, участвующие в процессах обработки персональных данных выполняют следующие функции:

 осуществляют взаимодействие с субъектами персональных данных по вопросам обработки их персональных данных;

 осуществляют уведомление субъектов персональных данных в случаях, определенных нормативными актами;

 эксплуатируют средства защиты персональных данных в соответствии с документацией на нее.

Сотрудники администрации Пугачевского муниципального района выполняют следующие функции:

 соблюдают требования нормативных документов по защите персональных данных;

 осуществляют обработку персональных данных в соответствии с заданием и предоставленными полномочиями.

# 14. Порядок организации и проведения работ по обеспечению безопасности персональных данных

Работы по обеспечению безопасности персональных данных при их обработке в ИСПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла ИСПДн, на следующих этапах:

инициация проекта ИСПДн;

планирование проекта ИСПДн;

реализация проекта ИСПДн, в составе:

выбор технического решения - концепция реализации;

проектирование ИСПДн;

производство ИСПДн;

приемка ИСПДн;

внедрение ИСПДн;

передача системы в эксплуатацию;

документирование проекта;

эксплуатация ИСПДн;

модернизация ИСПДн;

вывод из эксплуатации.

# 15. Контроль изменений в составе и структуре информационных систем персональных данных

Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться ответственным за обеспечение безопасности персональных данных.

Контролю подлежат следующие изменения:

внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);

изменение мест включения существующих компонентов ИСПДн;

удаление устройства из состава ИСПДн;

изменение мест установки устройства из состава ИСПДн;

прокладка новых кабельных линий связи и внешних линий связи или удаление старых кабельных линий связи;

существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке персональных данных;

создание новых и изменение существующих технологических процессов связанных с обработкой персональных данных.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн отслеживается и анализируется на предмет соответствия требованиям по защите ИСПДн. При необходимости производится модернизация системы защиты персональных данных.

# 16. Контроль за обеспечением необходимого уровня защищенности персональных данных

Для обеспечения эффективности процесса обеспечения безопасности персональных данных проводится:

контроль за соблюдением требований по обработке и защите персональных данных;

контроль за соблюдением условий использования средств защиты персональных данных, предусмотренных эксплуатационной и технической документацией;

контроль эффективности средств защиты персональных данных.

Контрольные мероприятия могут быть:

текущими;

плановыми внешними;

плановыми внутренними.

Ответственность за текущий контроль эффективности обеспечения безопасности персональных данных возлагается на администратора безопасности ИСПДн.

Ответственность за плановый контроль эффективности обеспечения безопасности персональных данных возлагается на ответственного за обеспечение безопасности персональных данных. Данные проверки должны включаться в план проверки информационной безопасности на год.

Для планового контроля эффективности средств защиты информации должны использоваться средства выявления уязвимостей информационной безопасности.

Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственного за обеспечение безопасности персональных данных.

При проведении контроля эффективности в общем случае должно проверяться:

наличие установленных средств защиты информации;

корректность настроек средств защиты информации;

выполнение пользователями и администраторами требований инструктивных материалов по защите персональных данных;

исполнение требований к процедурам обработки персональных данных (уничтожению персональных данных, сбору согласий, допуску персонала к персональным данным и т.п.);

правильность организации работы с носителями персональных данных;

соответствие системы защиты персональных данных реальному положению дел в администрации Пугачевского муниципального района.

# 17. Особенности организации обработки и хранения персональных данных, осуществляемых на материальных носителях, без использования средств автоматизации

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

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

Уточнение персональных данных при осуществлении их обработки производится путем обновления или изменения данных на бумажном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же бумажном носителе сведений о вносимых в них изменениях, либо путем изготовления нового бумажного носителя с уточненными персональными данными.

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

При несовместимости целей обработки персональных данных, зафиксированных на одном бумажном носителе, если бумажный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

Необходимо обеспечивать раздельное хранение документированной информации о персональных данных, обработка которых осуществляется в различных целях.

При обработке и хранении документированной информации должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

В помещения, где хранятся персональные данные, допускаются только сотрудники администрации Пугачевского муниципального района, получившие доступ к персональным данным и обрабатывающие персональные данные.

Порядок доступа муниципальных служащих администрации Пугачевского муниципального района в помещения, в которых ведется обработка персональных данных, утверждается распоряжением администрации Пугачевского муниципального района.

# 18. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Лица, виновные в нарушении требований законодательства Российской Федерации, регулирующего вопросы обработки и защиты персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Каждый пользователь информационных систем персональных данных администрации Пугачевского муниципального района, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

|  |  |
| --- | --- |
|  |  |

Приложение № 1
к Положению о порядке обработки персональных данных

Начат «\_\_\_» \_\_\_\_\_\_\_\_\_ \_\_\_\_ г.

Окончен «\_\_\_» \_\_\_\_\_\_\_\_\_ \_\_\_\_ г.

На \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ листах

# Журнал учета электронных носителей персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| Учетный номер | Датапостановки на учет | Вид электронного носителя,место его хранения (размещения) | Ответственный за использование и хранение |
| Ф.И.О. | подпись | дата |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |