Приложение 2

УТВЕРЖДЕНО

распоряжением администрации

муниципального образования

Ленинградский муниципальный округ Краснодарского края

от 15.07.2025 г. № 370-р

**Положение  
по обработке и защите информации ограниченного доступа,**

**не составляющей государственную тайну,**

**включая персональные данные**

**1. Общие положения**

1.1. Настоящее Положение по обработке и защите информации ограниченного доступа, не составляющей государственную тайну, включая персональные данные (далее - Положение, ИОД) разработано на основании Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа Роскомнадзора от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных», а также нормативных правовых актов и методических документов по вопросам безопасности персональных данных (далее - ПДн) при их обработке в информационных системах (далее - ИС), в том числе информационных системах персональных данных (далее - ИСПДн).

Настоящее Положение определяет политику администрации муниципального образования Ленинградский муниципальный округ Краснодарского края (далее - администрация) как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.2. В Положении используются следующие термины:

**информация** - сведения (сообщения, данные) независимо от формы их представления;

**информация ограниченного доступа (ИОД)** - информация, доступ к которой ограничен законодательством Российской Федерации;

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

**информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

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

**оператор ИС** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

**оператор ПДн** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

**обработка ПДн** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

**автоматизированная обработка ПДн** - обработка ПДн с помощью средств вычислительной техники;

**распространение информации (ПДн)** - действия, направленные на раскрытие информации (ПДн) неопределенному кругу лиц;

**предоставление информации (ПДн)** - действия, направленные на раскрытие информации (ПДн) определенному лицу или определенному кругу лиц;

**блокирование информации (ПДн**) - временное прекращение обработки информации (ПДн), за исключением случаев, если обработка необходима для уточнения ПДн;

**уничтожение информации (ПДн)** - действия, в результате которых становится невозможным восстановить содержание информации (ПДн) в ИС и (или) в результате которых уничтожаются материальные носители информации (ПДн);

**обезличивание ПДн** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

1.3. Настоящее Положение определяет порядок и условия обработки ИОД в администрации, включая порядок передачи ИОД третьим лицам, особенности автоматизированной и неавтоматизированной их обработки ИОД, порядок доступа к ИОД, систему защиты ИОД, порядок организации внутреннего контроля и ответственность за нарушения при обработке ИОД.

1.4. Требования к порядку обработки ИОД, указанные в настоящем Положении, предъявляются в том числе и к порядку обработки ПДн. При этом в отношении ПДн могут предъявляться дополнительные требования, указанные в отдельных пунктах Положения.

1.5. Действие настоящего Положения распространяется на все процессы обработки ИОД в администрации, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (в том числе передачу), блокирование, уничтожение ИОД, а также обезличивание ПДн, осуществляемые с использованием средств автоматизации и без их использования.

1.6. Все сотрудники администрации, участвующие в процессах обработки ИОД в администрации, должны быть ознакомлены с настоящим Положением в установленном порядке.

**2. Цели и задачи обработки ИОД**

2.1. Обработка ИОД осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей.

2.2. Обработка ИОД в администрации осуществляется в целях реализации возложенных на администрацию задач, исполнения функций и полномочий.

2.3. Особенности обработки ИОД, содержащей ПДн.

2.3.1. Не допускается обработка ПДн, несовместимая с заявленными целями сбора ПДн. Обработке подлежат только ПДн, которые отвечают целям их обработки.

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

2.3.3. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.3.4. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

2.3.5. Основными целями обработки ПДн является:

реализация возложенных на администрацию задач, исполнение муниципальных функций и полномочий администрации;

оказание государственных и муниципальных услуг (функций) на территории Ленинградского муниципального округа;

рассмотрение обращений и сообщений граждан;

ведение кадрового учета сотрудников администрации и лиц, не являющихся сотрудниками администрации.

2.3.6. ИСПДн обеспечивают решение следующих задач:

упрощение процедуры обработки ПДн, сокращение времени на их обработку;

контроль использования ПДн;

защита ПДн, в том числе воспрепятствование неправомерному доступу к ПДн;

объединение в единый формат и в единое хранилище данных, предоставленных субъектами, с учетом требований законодательства Российской Федерации;

обмен ПДн с использованием информационных систем связи и передачи информации.

**3. Информация ограниченного доступа,**

**обрабатываемая в администрации**

3.1. Перечень ИОД, обрабатываемой в администрации, указан в приложении 1 к настоящему распоряжению.

3.2. ПДн, обрабатываемые в администрации.

3.2.1. В администрации обрабатываются ПДн сотрудников администрации и лиц, не являющихся сотрудниками администрации.

3.2.2. ПДн субъектов ПДн могут включать:

специальные категории ПДн;

общедоступные ПДн;

иные категории ПДн.

Обработка биометрических ПДн в администрации не осуществляется.

3.2.3. Полные списки обрабатываемых ПДн формируются в перечнях ПДн, подлежащих защите (либо иных организационно-распорядительных документах), в ИСПДн администрации.

**4. Доступ к ИОД**

4.1. Сотрудники администрации, которые в силу выполняемых служебных обязанностей постоянно работают с ИОД, получают допуск к необходимой информации на срок выполнения ими соответствующих должностных обязанностей в соответствии с утвержденными перечнями лиц (должностей), допущенных к работе с ИОД.

4.2. Списки лиц (должностей), имеющих доступ к ИОД, должны поддерживаться в актуальном состоянии.

4.3. Администрацией установлен разрешительный порядок доступа к ИОД. Сотрудникам предоставляется доступ к работе с ИОД исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

4.4. В целях реализации возложенных на администрацию задач, исполнения функций и полномочий администрации отдельные функции обработки ИОД, могут осуществляться сотрудниками подведомственных администрации учреждений, с учетом требований законодательства Российской Федерации. В данном случае права и обязанности указанных сотрудников, связанные с обработкой ИОД и описанные в настоящем Положении, соответствуют правам и обязанностям сотрудников администрации.

4.5. Временный или разовый допуск к работе с ИОД в связи со служебной необходимостью может быть получен сотрудником администрации по согласованию с руководителями отраслевых (функциональных) и территориальных органов администрации без внесения изменений списка лиц (должностей), допущенных к работе с ИОД.

4.6. В случае если сотруднику сторонней организации требуется доступ к ИОД администрации, необходимо, чтобы в договоре со сторонней организацией (ином документе о взаимодействии между администрацией и сторонней организацией) были прописаны условия конфиденциальности ИОД и обязанность сторонней организации и ее сотрудников по соблюдению требований законодательства Российской Федерации в области обработки и защиты ИОД, а также, в случае передачи ПДн - обработки и защиты ПДн.

4.7. Доступ сотрудника администрации к ИОД прекращается с даты завершения трудовых отношений либо с даты изменения должностных обязанностей сотрудника и (или) исключения его из списков лиц, имеющих право доступа к ИОД. В случае увольнения все находившиеся в распоряжении сотрудника в соответствии с его должностными обязанностями носители, содержащие ИОД, передаются руководителям отраслевых (функциональных) и территориальных органов администрации.

4.8. Доступ к обрабатываемым в администрации ПДн со стороны третьих лиц (не являющихся сотрудниками администрации и подведомственных администрации учреждений) без согласия субъекта ПДн запрещен, если иное не определено законодательством Российской Федерации либо если передача ПДн третьим лицам необходима для достижения цели, на обработку ПДн для реализации которой получено согласие субъекта ПДн.

**5. Основные требования по защите ИОД**

5.1. При обработке ИОД в информационных системах администрации обеспечивается:

определением угроз безопасности ИОД при ее обработке в информационных системах;

проведением мероприятий, направленных на предотвращение несанкционированного доступа к ИОД и (или) передачи ее лицам, не имеющим права доступа к такой информации, в том числе применением организационных и технических мер по обеспечению безопасности ИОД;

применением средств защиты информации, имеющих сертификаты соответствия требованиям ФСТЭК России (для средств криптографической защиты информации - ФСБ России);

своевременное обнаружение фактов несанкционированного доступа к ИОД;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущением воздействия на технические средства обработки ИОД, в результате которого может быть нарушено их функционирование;

возможностью незамедлительного восстановления ИОД, модифицированной или уничтоженной вследствие несанкционированного доступа;

постоянным контролем обеспечения требований к защищенности ИОД и требуемого уровня защищенности ПДн (при наличии);

оценкой эффективности (аттестацией по требованиям информационной безопасности) принимаемых мер по обеспечению безопасности ИОД до ввода в эксплуатацию ИС и начала обработки ИОД в ней;

обнаружением фактов несанкционированного доступа к ИОД и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы и по реагированию на компьютерные инциденты в них;

восстановлением ИОД, модифицированной или уничтоженной вследствие несанкционированного доступа;

нахождением на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации.

5.2. Администрация принимает необходимые правовые, организационные и технические меры для обеспечения безопасности ИОД.

5.3. На основании нормативных правовых актов для установления требований по обеспечению безопасности и внедрения системы обеспечения безопасности ИОД в администрации разрабатывается комплект организационно-распорядительной документации.

В случае необходимости применения в ИС средств криптографической защиты информации (далее - СКЗИ) при разработке модели угроз также разрабатывается модель нарушителя информационной безопасности, в которой определяются требования к классам применяемых СКЗИ.

5.4. В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» членами комиссии по обследованию режимных помещений, категорированию и классификации объектов информатизации администрации, назначенными распоряжением администрации, проводится классификация ИС.

В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» членами комиссии по обследованию режимных помещений, категорированию и классификации объектов информатизации администрации, назначенными распоряжением администрации, проводится классификация (определение требуемого уровня защищенности обрабатываемых в ИСПДн ПДн) ИСПДн.

5.5. В соответствии с приказами ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (для ИСПДн) в администрации разрабатывается и внедряется комплекс мер по защите и обеспечению безопасности ИОД.

5.6. Все лица, допущенные к работе с ИОД, а также связанные с эксплуатацией и техническим сопровождением ИС, должны быть ознакомлены с требованиями настоящего Положения, а также должны соблюдать требования законодательства Российской Федерации в области защиты информации и обработки ПДн (в случае обработки ПДн).

5.8. Сотрудники администрации обязаны незамедлительно сообщать руководителям отраслевых (функциональных) и территориальных органов администрации об утрате или недостаче носителей ИОД, о причинах и условиях возможной утечки ИОД, о попытках посторонних лиц получить от сотрудника ИОД, обрабатываемую администрацией, а также о других случаях, создающих предпосылки для нарушения безопасности обрабатываемой в администрации ИОД.

**6. Порядок обработки и защиты ИОД**

6.1. Обязательным требованием для всех лиц, которым стала известна ИОД, обрабатываемая администрацией, является обеспечение ее конфиденциальности.

При необходимости при обработке ИОД также предъявляются требования по обеспечению ее целостности и доступности.

6.2. ИОД на бумажных носителях, обрабатываемые в администрации, хранятся в отраслевых (функциональных) и территориальных органах (у сотрудников), имеющих допуск к обработке соответствующей информации. Носители ИОД не должны оставаться без присмотра. При покидании рабочего места сотрудники, осуществляющие обработку ИОД, должны убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ИОД и (или) носителей ИОД осуществляется их восстановление (по возможности).

6.3. Порядок обращения с документами, изданиями (книгами, журналами, брошюрами, почтовыми отправлениями) и другими материальными и машинными носителями информации, содержащими ИОД, определяется Правилами делопроизводства в администрации, а также Положением о порядке учета, хранения и обращения со съемными носителями персональных данных и иной информации ограниченного доступа (приложение 3 к настоящему распоряжению).

6.4. При работе с программными средствами ИС администрации, реализующих функции просмотра и редактирования ИОД, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

6.5. При получении ИОД сотрудником администрации, который в соответствии с должностными обязанностями получает ИОД, в обязательном порядке проводится проверка достоверности ИОД. Ввод ИОД, полученной администрацией, в ИС, осуществляется сотрудниками, имеющими доступ к соответствующей информации.

При этом ввод и обработка ИОД допускается только в ИС, предназначенных для обработки такой информации.

6.6. Сотрудники, осуществляющие ввод ИОД в ИС, несут ответственность за достоверность и полноту введенной информации, а также за соблюдение требований информационной безопасности при вводе и обработке ими ИОД в ИС.

6.7. Обработка ПДн на бумажных носителях, без использования средств автоматизации (в случаях, если при обработке ПДн не используется ПЭВМ) осуществляется в соответствии с требованиями, утвержденными постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

6.7.1. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

6.7.2. При неавтоматизированной обработке ПДн на бумажных носителях не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых несовместимы между собой. При этом ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

6.8. Порядок уничтожения, блокирования и уточнения ИОД.

6.8.1. Уничтожение ИОД, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этой информации с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

6.8.2. Уточнение ИОД при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненной информацией.

6.8.3. По результатам уничтожения ПДн оформляется подтверждающий документ - акт об уничтожении ИОД в соответствии с приложением 12 к настоящему распоряжению.

6.8.4. В случае если подлежащая удалению ИОД содержит ПДн, обработка которых осуществляется с использованием средств автоматизации, кроме акта об уничтожении ИОД производится выгрузка из журнала регистрации событий в ИС.

6.8.5. Акт уничтожения ИОД подписывается комиссией. Акт об уничтожении ИОД подписывается членами комиссии.

6.8.6. Акт об уничтожении ИОД, а также (при наличии) выгрузка из журнала регистрации событий в ИСПДн подлежат хранению в течение 3 лет с момента уничтожения ИОД.

6.9. Уничтожение носителей, содержащих ИОД.

6.9.1. ИОД на бумажных носителях уничтожается путем использования шредеров (уничтожителей документов).

6.9.2. ИОД, размещенная на флэш-карте, CD-диске, ином носителе информации, уничтожается путем удаления содержимого носителя (форматирования носителя) или путем нарушения работоспособности флэш-карты или CD-диска.

6.9.3. По результатам уничтожении носителя информации составляется акт об уничтожении ИОД (приложение 12 к настоящему распоряжению).

6.10. По окончании рабочего дня сотрудники администрации закрывают в служебных помещениях, в которых могут храниться носители ИОД, окна, запирают данные помещения и включают сигнализацию (при наличии).

6.11. Сетевое оборудование, серверы, предназначенные для обработки ИОД, следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

6.12. Уборка помещений и обслуживание технических средств ИС должны осуществляться под контролем лиц, ответственных за данные помещения и (или) технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ИОД, носителям информации, программным и техническим средствам обработки, передачи и защиты информации в ИС.

6.13. В целях изучения и оценки фактического состояния защищенности ИОД, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения, в администрации осуществляется внутренний контроль процесса обработки ИОД.

Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ИОД направлены на решение следующих задач:

обеспечение соблюдения сотрудниками администрации требований настоящего Положения и нормативных правовых актов, регулирующих процессы обработки и защиты ИОД, обработки и защиты ПДн;

обеспечение работоспособности и эффективности технических средств ИС и средств защиты ИОД;

выявление нарушений установленного порядка обработки ИОД и своевременное предотвращение негативных последствий таких нарушений;

принятие корректирующих мер, направленных на устранение выявленных нарушений в процессе обработки ИОД и в работе технических средств ИС;

разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ИОД по результатам контрольных мероприятий;

осуществление внутреннего контроля исполнения рекомендаций и указаний по устранению нарушений.

Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ИОД, по модернизации технических средств ИС и средств защиты ИОД, по обучению и повышению компетентности персонала, задействованного в обработке ИОД.

6.14. В случае нарушения установленного порядка обработки ИОД сотрудники администрации несут ответственность в соответствии с разделом 9 настоящего Положения.

**7. Передача (предоставление) ИОД**

7.1. Предоставление ИОД или доступа к ним третьей стороне должны выполняться на основании:

законодательства Российской Федерации;

договора либо иного основания, существенным условием которого является обеспечение третьей стороной конфиденциальности ИОД и безопасности ИОД при ее обработке;

для ПДн - согласия субъекта ПДн на передачу его ПДн третьей стороне, за исключением случаев, когда такая передача необходима для достижения целей, на обработку ПДн в которых субъект ПДн ранее дал согласие, либо в случаях, когда в соответствии с законодательством Российской Федерации согласие субъекта ПДн на обработку его ПДн не требуется.

**8. Особенности обработки ИОД, содержащей ПДн,**

**в администрации**

8.1. Согласие на обработку ПДн.

8.1.1. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, по своей воле и в своих интересах. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством Российской Федерации. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются администрацией.

8.1.2. В случаях, когда в соответствии с требованиями законодательства обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн, равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

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

фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;

цель обработки ПДн;

перечень ПДн, на обработку которых дается согласие субъекта ПДн;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;

перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

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

подпись субъекта персональных данных.

8.1.3. Требования пункта 8.1.2 настоящего Положения не распространяются на случаи, когда письменная форма согласия субъекта ПДн на обработку его ПДн выбрана администрацией как оператором ПДн, но не является обязательной согласно требованиям законодательства Российской Федерации.

8.1.4. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн администрация вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, предусмотренных законодательством Российской Федерации.

8.1.5. Получение согласия на обработку ПДн осуществляется сотрудником при получении ПДн от субъекта ПДн путем оформления согласия по форме, установленной в приложении 9 к настоящему распоряжению, за исключением случаев, указанных в пункте 8.1.2 настоящего Положения.

8.1.6. Если в соответствии с законодательством Российской Федерации предоставление ПДн и (или) получение администрацией согласия на обработку ПДн являются обязательными, администрация обязана разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку.

8.2. Права субъекта в отношении ПДн, обрабатываемых администрацией.

8.2.1. Субъект ПДн имеет право:

получать от администрации информацию, касающуюся обработки его ПДн в установленном законодательством Российской Федерации порядке. Сведения должны быть предоставлены субъекту ПДн в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта ПДн или его представителя в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления администрацией в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Перечень сведений и порядок получения сведений предусмотрен законодательством Российской Федерации;

обращаться в администрацию по вопросу уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав;

обращаться в администрацию с отзывом ранее данного администрации согласия на обработку его ПДн. При этом такое обращение должно содержать информацию, на основании которой администрация может однозначно определить субъекта ПДн и ПДн, на обработку которых субъект ПДн отзывает согласие;

давать предварительное письменное согласие при принятии администрацией исключительно в процессе автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы;

заявлять возражения на решения администрации в процессе исключительно автоматизированной обработки ПДн и на возможные юридические последствия таких решений;

обжаловать действия или бездействие администрации в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

8.3. Права и обязанности администрации при обработке ПДн.

8.3.1. Администрация вправе:

поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия соответствующего акта, в порядке, предусмотренном законодательством Российской Федерации;

в случае отзыва субъектом ПДн согласия на обработку ПДн продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, предусмотренных законодательством Российской Федерации;

отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством Российской Федерации. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на администрации;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей администрации, предусмотренных законодательством Российской Федерации.

8.3.2. Администрация обязана:

уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн;

назначить должностное лицо, ответственное за организацию обработки ПДн;

при сборе ПДн, обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных законодательством Российской Федерации;

разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку, если предоставление ПДн и (или) получение администрацией согласия на обработку ПДн являются обязательными;

при получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации;

представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований обработки ПДн без согласия субъекта ПДн;

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

при сборе ПДн предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством Российской Федерации;

опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику администрации в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПД;

принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей администрации, предусмотренных законодательством Российской Федерации;

представить документы и локальные акты, предусмотренные законодательством Российской Федерации, и (или) иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей администрации по запросу уполномоченного органа по защите прав субъектов ПДн;

при обработке ПДн принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

ознакомить сотрудников администрации, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику администрации в отношении обработки ПДн, локальными актами администрации по вопросам обработки ПДн;

исполнять иные обязанности, предъявляемые к операторам ПДн законодательством Российской Федерации.

8.4. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», договором, стороной которого является субъект ПДн.

8.6. В целях информационного обеспечения в администрации могут создаваться специализированные справочники (телефонные, адресные книги и др.), содержащие ПДн, к которым с письменного согласия субъекта ПДн может предоставляться доступ неограниченному кругу лиц. Сведения о субъекте ПДн должны быть незамедлительно исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

**9. Ответственность за нарушение законодательства**

**в области обработки и защиты ИОД,**

**обработки и защиты ПДн**

9.1. Начальники отраслевых (функциональных) и территориальных органов администрации несут ответственность за необеспечение конфиденциальности ИОД, за несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

9.2. Сотрудники администрации несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ИОД, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

9.3. Сотрудник администрации может быть привлечен к ответственности в случаях:

умышленного или неумышленного раскрытия либо искажения ИОД;

утраты материальных носителей ИОД;

нарушения требований настоящего Положения и других нормативных документов администрации в части вопросов доступа и работы с ИОД;

нарушения установленного порядка обработки и обеспечения безопасности ИОД, несанкционированного доступа к ИОД, раскрытия ИОД и нанесения администрации, его сотрудникам, субъектам обрабатываемых в администрации ПДн материального или морального ущерба.

Управляющий делами

администрации Ленинградского

муниципального округа А.Л. Мазуров