

**ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ,
ОБРАБАТЫВАЕМЫХ В МУНИЦИПАЛЬНОМ УНИТАРНОМ ПРЕДПРИЯТИИ
Г. АСТРАХАНИ «АСТРВОДОКАНАЛ»**

1. Общие положения

- 1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Жилищным Кодексом Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», другими федеральными законами и нормативными актами, регулирующими вопросы защиты конфиденциальной информации.
- 1.2. Цель разработки Положения – определение порядка обработки и защиты персональных данных в муниципальном унитарном предприятии г. Астрахани «Астрводоканал» (далее - Предприятие), закрепление ответственности сотрудников, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. Основные понятия

Для целей настоящего Положения используются следующие основные понятия:

- 2.1. **Работник Предприятия** — лицо, вступившее в трудовые отношения с Предприятием (далее – работник, сотрудник);
- 2.2. **Персональные данные** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, необходимая Предприятию в связи с трудовыми отношениями/при оказании коммунальных услуг;
- 2.3. **Персональные данные специальной категории** — персональные данные, касающиеся состояния здоровья;
- 2.4. **Общедоступные персональные данные** — служебные персональные данные, доступ к которым неограничен и на которые не распространяется требование соблюдения конфиденциальности в связи с отсутствием негативных последствий для субъекта персональных данных в случае их раскрытия;
- 2.5. **Обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание,
- 2.6. **Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники;
- 2.7. **Неавтоматизированная обработка персональных данных** — обработка персональных данных без помощи средств вычислительной техники;
- 2.8. **Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 2.9. **Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 2.10. **Блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 2.11. **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;

- 2.12. **Обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 2.13. **Информационная система персональных данных** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 2.14. **Конфиденциальность персональных данных** — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работника, требование не допускать их распространения без согласия работника или иного законного основания;

3. Состав и принципы обработки персональных данных

- 3.1. Предприятие не имеет право получать и обрабатывать персональные данные работника, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, членства в общественных объединениях или его профсоюзной деятельности.
- 3.2. В состав персональных данных, обрабатываемых Предприятием, входит комплекс документов, сопровождающий процесс оформления трудовых отношений с работником в Предприятии при его приеме, назначении, переводе и увольнении, а также процесс оказания коммунальных услуг гражданам.
- 3.3. Предприятием определен перечень сведений конфиденциального характера, согласно которому происходит обработка следующих категорий персональных данных:
- Персональные данные работников Предприятия.
 - Персональные данные абонентов, к которым Предприятие получает доступ в рамках своей основной деятельности – реализации коммунальных услуг.
- 3.4. Лицо, подписывающее трудовой договор/договор на оказание услуг по организации сбора и учета платежей за ВКУ с Предприятием автоматически соглашается с тем, что его персональные данные будут обрабатываться Предприятием в соответствии с настоящим Положением. Работник Предприятия, в том числе признает тот факт, что он не возражает против того, что некоторые данные (указанные в Приложении 1) станут общедоступными и доступ к ним не будет ограничен.
- 3.5. Перечень персональных данных работника, необходимый для оформления трудовых отношений, определяется Трудовым Кодексом Российской Федерации;
- 3.6. Для публикации (размещения в общедоступном источнике) персональных данных работников, помимо отнесенных к общедоступным, необходимо получение согласия субъекта персональных данных. Образец согласия приведен в Приложении № 4 настоящего Положения.
- 3.7. Общедоступные персональные данные могут обрабатываться всеми сотрудниками Предприятия в автоматизированном и неавтоматизированном виде без установления требований по обеспечению безопасности информации. Обеспечение целостности указанных сведений осуществляется при необходимости.
- 3.8. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом

затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством.

3.9. В целях обеспечения прав и свобод человека и гражданина Предприятие и ее представители при обработке персональных данных обязаны соблюдать следующие общие правила:

- Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности работника, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера заработной платы, предоставления гражданину коммунальных услуг;
- Обработка персональных данных граждан (в том числе работников Предприятия) может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- При определении объема и содержания, обрабатываемых персональных данных, Предприятие должно руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;
- Получение персональных данных Предприятием может осуществляться как путем представления их самим субъектом персональных данных, так и путем получения их у третьей стороны;
- Если персональные данные возможно получить только у третьей стороны, субъект персональных данных должен быть уведомлен об этом не менее чем за три рабочих дня, и от него должно быть получено письменное согласие (либо письменный отказ), которое он должен дать в течение пяти рабочих дней с момента получения соответствующего уведомления. В письменном уведомлении Предприятие должно сообщить гражданину о цели обработки персональных данных и ее правовое обоснование, предполагаемых пользователях персональных данных, источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение;
- Защита персональных данных от неправомерного их использования или утраты обеспечивается Предприятием за счет его средств в порядке, установленном федеральными законами.

4. Порядок получения Предприятием персональных данных

- 4.1. Сотрудник отдела кадров обязан ознакомить работника с настоящим Положением под подпись до заключения трудового договора.
- 4.2. Лицо, поступающее на работу в Предприятие, оформляет письменное согласие на обработку Предприятием его персональных данных. Образец согласия приведен в Приложении № 3 настоящего Положения.
- 4.3. При заключении договора на оказание услуг по организации сбора и учета платежей за ВКУ с Предприятием абонент вправе ознакомиться с настоящим Положением. В договоре абонент заверяет личной подписью факт согласия на обработку его персональных данных.
- 4.4. В целях обеспечения достоверности персональных данных гражданин обязан предоставить в Предприятие комплекс достоверных, документированных персональных данных, состав которых установлен Законодательством РФ. Уполномоченный сотрудник Предприятия проверяет достоверность данных,

представленных гражданином, с имеющимися у гражданина подлинными документами.

- 4.5. В случае изменения персональных данных в процессе трудовых отношений гражданин обязан письменно уведомить Предприятие о таких изменениях и предоставить изменившиеся данные в разумные сроки.
- 4.6. По мере необходимости, обусловленной спецификой выполняемых трудовых функций работника Предприятие вправе требовать от него предоставления дополнительных сведений, содержащих персональные данные. Гражданин представляет необходимые, достоверность которых проверяется сотрудником отдела кадров.
- 4.7. Запрещается требовать от субъекта персональных данных предоставления персональных данных, кроме предусмотренных Трудовым Кодексом Российской Федерации, федеральными законами, указами Президента Российской Федерации, и т.п.
- 4.8. В случае, если юридические и физические лица (далее - контрагенты) на основании заключенных договоров (либо иных оснований) оказывают услуги Предприятию, и в силу данных договоров они должны иметь доступ к персональным данным сотрудников/абонентов Предприятия, то соответствующие данные предоставляются Предприятием только после подписания с контрагентами обязательства о неразглашении персональных данных, в объемах необходимых для осуществления условий соответствующего договора

5. Хранение персональных данных работников

- 5.1. Персональные данные работников, представляют собой совокупность документов, сопровождающую процесс оформления трудовых отношений работника в Предприятии при его приеме, переводе и увольнении.
- 5.2. Ответственный за организацию обработки и защиты персональных данных назначается приказом генерального директора.
- 5.3. Перечень персональных данных, обрабатываемых в информационных системах, утверждается приказом генерального директора.
- 5.4. Персональные данные Предприятия в неавтоматизированном виде должны храниться в местах, исключающих несанкционированный доступ: запираемых шкафах, сейфах, хранилищах и т.п. Ответственность за хранение персональных данных Предприятия несут начальники структурных подразделений, в которых происходит обработка персональных данных.
- 5.5. При достижении целей обработки персональные данные подлежат уничтожению в срок, не превышающий тридцати дней с даты достижения таких целей. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Предприятие осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.
Требование об уничтожении не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения трудовых отношений.

6. Передача персональных данных

- 6.1. Передача персональных данных Предприятия третьей стороне должна осуществляться только при условии обязательного выполнения требования конфиденциальности.
- 6.2. При передаче персональных данных субъектов сотрудники Предприятия, имеющие доступ к персональным данным, должны осуществлять передачу в соответствии с настоящим Положением и действующим законодательством РФ.

- 6.3. От лица, чьи персональные данные передаются третьей стороне, должно быть получено согласие на передачу этих данных. Образец согласия приведен в Приложении №5.
- 6.4. Персональные данные субъекта не должны быть переданы третьей стороне без его письменного согласия, за исключением следующих случаев:
 - 6.4.1. осуществляется передача общедоступных персональных данных;
 - 6.4.2. передача персональных данных осуществляется при условии обязательного обезличивания персональных данных;
 - 6.4.3. передача персональных данных является требованием действующего федерального закона или договора между работником и Предприятием;
 - 6.4.4. передача персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение их согласия невозможно, а также передача персональных данных необходима для прохождения медицинской комиссии работника.
 - 6.4.5. указанных в пунктах 6.9 – 6.11 настоящего Положения.

Учитывая, что Федеральный закон «О персональных данных» не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта персональных данных, Предприятие в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же третья сторона, обратившаяся с запросом, не уполномочена федеральным законом на получение персональных данных, либо отсутствует письменное согласие на предоставление персональных сведений гражданина, либо, по мнению Предприятия, отсутствует угроза жизни или здоровью, Предприятие обязано отказать в предоставлении персональных данных гражданина третьей стороне.
- 6.5. При передаче персональных данных третьей стороне должны быть переданы только те данные, которые необходимы для достижения целей обработки, а также на которые было получено согласие работника.
- 6.6. Решение о передаче персональных данных третьей стороне рассматривается генеральным директором. При принятии решения ему необходимо руководствоваться законодательством РФ и настоящим Положением. В случае если законность передачи персональных данных третьей стороне вызывает сомнения, генеральный директор обращается к ответственному за обработку и защиту персональных данных для получения необходимых разъяснений.
- 6.7. Третья сторона, получившая персональные данные от Предприятия, должно быть предупреждена, что эти данные могут быть использованы лишь в целях, для которых они были переданы.
- 6.8. Передача персональных данных работников/абонентов в ответ на запросы третьей стороны на бумажных носителях осуществляется в соответствии с «Регламентом по обработке запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных».
- 6.9. В случае передачи персональных данных работников/абонентов на бумажных носителях, кроме указанного в п.6.8 настоящего Положения, факт передачи должен фиксироваться в соответствии с принятыми на Предприятии правилами документооборота (при этом должна быть возможность отследить время передачи; адресата; сотрудника, осуществившего передачу).
- 6.10. При передаче персональных данных на электронных носителях сотрудник, осуществляющий соответствующую передачу, должен зарегистрировать в канцелярии сопроводительный документ к передаваемому носителю. Формирование и регистрация сопроводительного документа производится в соответствии с принятыми на Предприятии правилами документооборота.
- 6.11. В целях открытия лицевых счетов и зачисления денежных средств необходимые персональные данные сотрудников Предприятия передаются в

электронном виде в Банк, выполняющий операции перечисления денежных средств на счета банковских карт сотрудников Предприятия. Договор, заключенный с Банком, обязывает стороны соблюдать конфиденциальность и безопасность персональных данных сотрудников Предприятия.

- 6.12. Бухгалтер расчетной части бухгалтерии Предприятия отправляет электронные отчетности, содержащие персональные данные работников:
- 6.12.1. в Пенсионный фонд Российской Федерации в соответствии с ФЗ № 27 от 1 апреля 1996 г. «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» с использованием средства криптографической защиты информации (далее – СКЗИ);
 - 6.12.2. в Инспекцию Федеральной налоговой службы согласно Налоговому Кодексу Российской Федерации с использованием СКЗИ;
 - 6.12.3. в Фонд социального страхования Российской Федерации в соответствии с ФЗ № 212-ФЗ от 24.07.2009 «О страховых взносах в пенсионный фонд Российской Федерации, фонд социального страхования Российской Федерации, федеральный фонд обязательного медицинского страхования» с использованием системы СКЗИ.
- 6.13. Согласно договору, заключенному между Предприятием и ООО «Социальные гарантии» (далее – Соц. Гарантии) в целях обслуживания лицевого счета абонентов, необходимые персональные данные последних передаются в электронном виде в Соц. Гарантии посредством защищенного канала связи. Договор обязывает стороны соблюдать конфиденциальность и безопасность персональных данных абонентов Предприятия.

7. Обеспечение безопасности персональных данных

- 7.1. При обработке персональных данных (как при автоматизированной, так и при неавтоматизированной) в Предприятии соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.
- 7.2. Перечень лиц Предприятия, имеющих доступ к персональным данным работников и абонентов Предприятия, утверждается приказом генерального директора.
- 7.3. Перед получением доступа к персональным данным сотрудник Предприятия подписывает обязательство о неразглашении информации, содержащей персональные данные, согласно Приложению № 2 настоящего Положения. Для сотрудника Предприятия, получившего доступ к персональным данным, обязательным является требование не допускать распространение данной информации без согласия работника/абонента, а также без иного законного основания.
- 7.4. Сотрудники Предприятия, получившие доступ к персональным данным, для соблюдения режима конфиденциальности должны руководствоваться требованиями настоящего Положения, своих должностных инструкций, а также прочих локальных организационно-распорядительных документов Предприятия.
- 7.5. Обо всех фактах и попытках нарушения безопасности персональных данных сотрудники Предприятия обязаны ставить в известность руководителя структурного подразделения, в котором произошел инцидент, ответственного за организацию обработки и защиты персональных данных, а также отдел информационных технологий и коммуникаций.
- 7.6. При передаче персональных данных третьей стороне должен использоваться безопасный канал передачи. Запрещается передавать персональные данные (кроме общедоступных) через сеть международного информационного обмена (отправлять по электронной почте и т.п.) без применения необходимых

программных и/или аппаратных средств защиты. За организацию безопасного канала передачи персональных данных третьей стороне отвечает группа информационной безопасности и системного администрирования отдела информационных технологий и коммуникаций.

- 7.7. Отдел информационных технологий и коммуникаций Предприятия совместно с ответственным за организацию обработки и защиты персональных данных контролируют соблюдение требований федеральных законов по защите персональных данных и организывает мероприятия по их реализации. Отдел информационных технологий и коммуникаций Предприятия обеспечивает техническое обслуживание и сопровождение средств защиты персональных данных.
- 7.8. Электронные носители информации, содержащие персональные данные работников, учитываются в журналах учета электронных носителей персональных данных для каждой информационной системы, ответственными за ведение которых являются администратор безопасности.
- 7.9. Съёмные электронные носители информации, содержащие персональные данные, хранятся в служебных помещениях в надёжно запираемых шкафах. При этом создаются надлежащие условия, обеспечивающие их сохранность. Правила работы со съёмными носителями, содержащими персональные данные, закреплены локальными организационно-распорядительными документами, за разработку которых отвечает администратор безопасности информации.

8. Права гражданина в целях защиты персональных данных

- 8.1. В целях обеспечения защиты персональных данных, хранящихся у Предприятия, работники имеют право на:
 - 8.1.1. Свободный бесплатный доступ ко всем своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
 - 8.1.2. Определение законных представителей для защиты своих персональных данных;
 - 8.1.3. Исключение или исправление по письменному требованию неверных или неполных персональных данных, а также данных, обработанных с нарушением требований федерального закона. При отказе Предприятия исключить или исправить персональные данные работника он имеет право заявить в письменной форме Предприятию о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
 - 8.1.4. Обжалование в судебном органе любых неправомерных действий или бездействия Предприятия при обработке и защите его персональных данных.
 - 8.1.5. Доступ работника/абонента к его персональным данным предоставляется ему или его законному представителю Предприятия при обращении либо при получении запроса работника/абонента или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность работника/абонента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, собственноручную подпись работника или его законного представителя. К запросу должен быть приложен документ, подтверждающий полномочия законного представителя.

9. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных

- 9.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.
- 9.2. Генеральный директор Предприятия, разрешая передачу персональных данных третьей стороне, несет персональную ответственность за данное разрешение в соответствии с законодательством Российской Федерации.

Разработано:

Инженер 1 категории по информационной безопасности

отдела ИТиТ


_____ Ахмедова А.Г.

« 20 » _____ 10 2016г.