

УТВЕРЖДАЮ

Начальник управления закупок
администрации муниципального
образования город Краснодар

С.В.Мартынов

2016 года



ПОЛИТИКА

обработки персональных данных управления закупок администрации муниципального образования город Краснодар

1. Общие положения

Настоящая Политика обработки персональных данных (далее – Политика):

– является внутренним документом управления закупок администрации муниципального образования город Краснодар (далее – Управление), регулирующим вопросы обработки персональных данных;

– разработана в целях обеспечения обработки, хранения и защиты ПДн работников Управления в соответствии с законодательством Российской Федерации;

– раскрывает основные категории персональных данных, обрабатываемых Управлением, цели, способы и принципы их обработки, права и обязанности работников Управления при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Управлением в целях обеспечения безопасности персональных данных при их обработке;

– предназначена для работников Управления, осуществляющих обработку персональных данных, в целях непосредственной реализации ими закреплённых в Политике принципов. Является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Управления при обработке персональных данных.

2. Источники нормативного правового регулирования вопросов обработки персональных данных

2.1. Политика Управления в области обработки персональных данных определяется на основании следующих нормативных правовых актов Российской Федерации:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации»;
- Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое Постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждённые Постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации;
- Нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора.

2.2. Во исполнение настоящей Политики в Управлении утверждаются следующие локальные акты:

- Положение о защите, хранении, обработке и передаче персональных данных работников Управления;
- Инструкция администратора сети и информационной системы персональных данных;
- Инструкция администратора безопасности информационной системы персональных данных;
- Инструкция оператора автоматизированного рабочего места информационных систем персональных данных;
- Инструкция по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций;
- Инструкция по защите от воздействия программных вирусов информационных систем персональных данных;
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- План внутренних проверок состояния защиты информации в Управле-

нии;

- Перечень персональных данных, обрабатываемых в Управлении;
- План мероприятий по защите информации в Управлении;
- Правила обработки персональных данных в Управлении;
- Акт классификации информационных систем персональных данных Управления;
- Модель угроз Управления;
- и иные локальные документы Управления, принимаемые во исполнение требований действующих нормативных правовых актов Российской Федерации в области обработки персональных данных.

3. Основные термины и понятия, используемые в локальных документах управления, принимаемых по вопросу обработки персональных данных

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в Управлении локальными актами Управления.

Обработка персональных данных – 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.

Распространение персональных данных – действия, направленные на раскрытие ПДн неопределённому кругу, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

Предоставление персональных данных – действия, направленные на раскрытие ПДн определённому кругу.

Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной

системе персональных данных и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

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

Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

4. Общие условия обработки персональных данных

4.1. Обработка ПДн в Управлении осуществляется на основе следующих принципов:

4.1.1. Законности и справедливости обработки ПДн.

4.1.2. Законности целей и способов обработки ПДн и добросовестности.

4.1.3. Соответствия целей обработки ПДн целям, заранее определённым и заявленным при сборе ПДн, а также полномочиям управления.

4.1.4. Соответствия содержания и объёма обрабатываемых ПДн целям обработки ПДн.

4.1.5. Достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.

4.1.6. Недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.8. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.9. Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Управлению своих ПДн.

4.1.10. Держателем ПДн является Управление, которому субъект ПДн передаёт во владение свои ПДн. Управление выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

4.1.11. Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и обеспечивает безопасность информации в процессе деятельности Управления.

4.1.12. Управление при обработке ПДн обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИС.

4.1.13. Мероприятия по защите ПДн определяются Положением, приказами, инструкциями и другими внутренними документами управления.

4.2. Для защиты ПДн в Управлении применяются следующие принципы и правила:

4.2.1. Ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн.

4.2.2. Строгое избирательное и обоснованное распределение документов и информации между работниками.

4.2.3. Рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации.

4.2.4. Знание работниками требований нормативно-методических документов по защите ПДн.

4.2.5. Распределение персональной ответственности между работниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн.

4.2.6. Установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных.

4.2.7. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

4.2.8. Исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведётся обработка ПДн и находится соответствующая вычислительная техника.

4.2.9. Организация уничтожения носителей персональных данных.

4.2.10. Своевременное выявление нарушений требований разрешительной системы доступа.

4.2.11. Разъяснительная работа с работниками Управления по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

4.2.12. Регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

4.2.13. Ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.

4.2.14. Создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

- 4.2.15. Резервирование защищаемых данных (создание резервных копий).
- 4.3. Цели обработки персональных данных:
 - 4.3.1. Ведение кадрового и бухгалтерского учёта работников Управления.
 - 4.3.2. Отправка отчётности по кадровому и бухгалтерскому учёту.

Начальник отдела организационно-
правового и финансового обеспечения
управления закупок администрации
муниципального образования
город Краснодар

 В.В.Сергейко