

## ПОЛОЖЕНИЕ

об основных направлениях деятельности (политике) Муниципального казенного учреждения «Служба заказчика Верх-Исетского района города Екатеринбурга» в области обработки персональных данных

### Глава 1. Общие положения

1.1. Положение об основных направлениях в деятельности (политике) Муниципального казенного учреждения «Служба заказчика Верх-Исетского района города Екатеринбурга» (далее – Учреждение) в области обработки персональных данных - основополагающий внутренний нормативный документ, определяющий порядок обработки персональных данных и выполнение требований по обеспечению их безопасности.

1.2. Положение разработано в соответствии с законодательством Российской Федерации в области обработки и обеспечения безопасности персональных данных: Конституцией Российской Федерации; Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»; Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Уставом муниципального образования «город Екатеринбург» (ст. 8 - 10, 36, 37), утвержденным Решением Екатеринбургской городской Думы от 30.06.2005 № 8/1; иными нормативными правовыми актами в области обработки и обеспечения безопасности персональных данных, а также документами ФСТЭК России и ФСБ России.

В настоящем Положении используются следующие основные понятия:

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту 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.

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, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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.

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

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.

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

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

## Глава 2. Обработка персональных данных

### 2.1. Основные принципы обработки персональных данных:

законность;

целевой характер;

точность;

актуальность;

удаление или уточнение неполных (неточных) данных.

2.2. В процессе исполнения своих полномочий Учреждение обрабатывает персональные данные следующих субъектов: сотрудники, с которыми заключены трудовые договоры; их близкие родственники; граждане, обратившиеся в Учреждение с жалобами, заявлениями; граждане, направившие резюме при устройстве на работу; физические лица, состоящие в договорных или иных гражданско-правовых отношениях.

Биометрические персональные данные в Учреждении не обрабатываются.

Трансграничная передача персональных данных не производится.

2.3. Обработка персональных данных в Учреждении осуществляется с соблюдением следующих условий:

1) они должны быть получены от субъекта персональных данных или его законного представителя;

2) для обработки персональных данных необходимо: получение согласия каждого субъекта, персональные данные которого обрабатываются; получение согласия на передачу (предоставление) персональных данных третьим лицам (согласие на обработку его персональных данных не требуется в случаях, предусмотренных законодательством Российской Федерации);

3) при передаче (предоставлении) персональных данных одним оператором Учреждением другому в рамках предоставления муниципальной (государственной) услуги оба оператора применяют организационные и технические меры по обеспечению безопасности как переданных, так и полученных персональных данных;

4) передача (предоставление) персональных данных оператором (Учреждение) стороннему оператору осуществляется на основании договора, обязательным условием которого является обеспечение их безопасности.

2.4. Сроки хранения носителей персональных данных и их электронных копий определяются распорядительными актами. Порядок уничтожения носителей устанавливается соответствующей инструкцией.

2.5. Субъект персональных данных (далее - субъект) имеет право на получение информации, касающейся обработки его персональных данных, в том

числе содержащей: подтверждение факта обработки персональных данных; правовые основания и цели обработки персональных данных; цели и способы обработки персональных данных, применяемых в Учреждении; наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом; сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом своих законных прав; информацию об осуществленной или о предполагаемой трансграничной передаче данных; фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные законодательством.

Субъект вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Если субъект считает, что оператор нарушает его права и свободы, он вправе обжаловать действия или бездействие оператора в орган по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций — Роскомнадзор) или в судебном порядке.

Субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке, а также иные права, предусмотренные законодательством.

### Глава 3. Правовые, организационные и технические меры, принимаемые Учреждением для обеспечения безопасности обрабатываемых персональных данных

3.1. Учреждением принимаются следующие правовые меры: утверждается система обеспечения безопасности персональных данных при их обработке в информационных системах; разрабатываются требования по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных; составляется реестр информационных систем персональных данных; определяются требования по организации и обеспечению функционирования шифровальных (криптографических) средств; утверждается типовое обязательство (раздел трудового контракта) работника Учреждения, осуществляющего обработку персональных данных; назначается ответственный пользователь шифровальных (криптографических) средств; разрабатывается ежегодный план проверок выполнения требований по защите персональных данных при их обработке в информационных системах.

3.2. Принимаются организационные меры по обеспечению безопасности персональных данных:

1) отправляется уведомление в уполномоченный орган по защите прав субъектов об обработке персональных данных;

2) создается комиссия по классификации информационных систем персональных данных;

3) разрабатываются правила работы с обезличенными данными;

4) назначаются: лицо, ответственное за обеспечение безопасности персональных данных; лица, ответственные за эксплуатацию информационных систем персональных данных;

5) определяются: помещения для обработки персональных данных и правила доступа в них; правила внутреннего контроля соответствия обработки персональных данных требованиям к их защите, установленным законодательством;

6) утверждаются документы: список работников, доступ которых к персональным данным в информационных системах персональных данных необходим для выполнения служебных (трудовых) обязанностей; перечень персональных данных, подлежащих защите; правила рассмотрения запросов субъектов персональных данных или их представителей; перечень должностей Учреждения, ответственных за проведение мероприятий по обезличиванию персональных данных; должностная инструкция ответственного за обеспечение безопасности персональных данных; типовая форма согласия на обработку персональных данных работников Учреждения и иных субъектов, а также типовая форма разъяснения субъекту юридических последствий отказа предоставить свои персональные данные;

7) выполняются требования по обработке персональных данных, осуществляемой без использования средств автоматизации.

3.3. На каждую информационную систему персональных данных разрабатывается Модель угроз безопасности, на основании которой строится система защиты на основе следующих принципов: законность, системность,

предоставить свои персональные данные;

7) выполняются требования по обработке персональных данных, осуществляемой без использования средств автоматизации.

3.3. На каждую информационную систему персональных данных разрабатывается Модель угроз безопасности, на основании которой строится система защиты на основе следующих принципов: законность, системность, своевременность, комплексный подход, непрерывность защиты, преемственность и совершенствование, минимизация полномочий, разумная достаточность (экономическая целесообразность), персональная ответственность, обоснованность и реализуемость, гибкость системы защиты, профессионализм, обязательность контроля.

3.4. На всех персональных компьютерах, входящих в состав информационных систем персональных данных, устанавливаются только учтенные сертифицированные средства защиты информации.

3.5. Объекты защиты персональных данных: персональные данные, обрабатываемые и хранящиеся на персональных компьютерах работников, серверах, на отчуждаемых (съемных) носителях информации; персональные данные, передаваемые по каналам связи; персональные данные, хранящиеся в документированном виде на бумажных носителях; прикладное и системное программное обеспечение персональных компьютеров, серверов, используемых для обработки персональных данных; оборудование серверов, персональные компьютеры, коммуникационное оборудование; средства защиты информации информационных систем персональных данных (в том числе шифровальные (криптографические) средства защиты информации); съемные машинные носители информации - накопители на жестких магнитных дисках, Flash-накопители, оптические диски (CD, DVD, -R, -RW).

В Учреждении установлена сигнализация. Доступ в помещения, в которых ведется обработка персональных данных, посетителей производится исключительно в присутствии работников, исполняющих в данных помещениях свои должностные обязанности.

#### Глава 4. Заключительные положения

4.1. Учреждение несет ответственность за нарушение обязательств по обеспечению безопасности и конфиденциальности персональных данных при их обработке в соответствии с законодательством Российской Федерации.