Приложение
к приказу управления
от 04.04.2016г. № 40-ОД

Политика
в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных Управления государственных закупок Тюменской области

1.Общие положения

1. Настоящий документ «Политика в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных Управления государственных закупок Тюменской области» (далее - Политика) определяет высокоуровневую политику в отношении обработки персональных данных субъектов и содержит сведения о реализуемых требованиях к защите персональных данных в Управлении государственных закупок Тюменской области (далее – управление).

2. Настоящая Политика разработана на основе действующих правовых и нормативных документов по защите конфиденциальной информации и персональных данных.

3. Под персональными данными в настоящем документе понимается любая информация, относящаяся к прямо или косвенно, определенному или определяемому физическому лицу (субъекту персональных данных).

4. Настоящая Политика утверждается приказом управления.

5.Согласно статье 18.1, п.2 Федерального закона от 25.07.2006 г. № 152 ФЗ «О персональных данных» управление, как оператор персональных данных, обязано 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.

6.Управление в рамках выполнения своей деятельности осуществляет обработку персональных данных и, в соответствии с действующим законодательством Российской Федерации, является оператором персональных данных с соответствующими правами и обязанностями, определенными Федеральным законом № 152 от 27.07.2006 «О персональных данных» и иными нормативными правовыми актами Российской Федерации (далее - РФ). Состав обрабатываемых данных, категории субъектов, чьи персональные данные обрабатываются управлением, цели и правовые основания их обработки закреплены для каждой информационной системы управления «Перечнем персональных данных, обрабатываемых в ИСПДН».

2. Принципы, правила и цели обработки персональных данных

2.1.Обработка персональных данных осуществляется управлением с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 г. № 152 ФЗ «О персональных данных»:

-обработка персональных данных осуществляется на законной и справедливой основе;

-обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

-не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

-не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

-обработке подлежат только персональные данные, которые отвечают целям их обработки;

-содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;

-обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

-управление принимает все необходимые меры по предотвращению разглашения и нарушения конфиденциальности персональных данных;

-при обработке персональных данных управление обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

-управление принимает необходимые меры по удалению или уточнению неполных или неточных данных;

-хранение персональных данных в управлении осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, к примеру Федеральным законом от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» или договором, стороной которого является субъект персональных данных;

-обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

2.2.Обработка персональных данных осуществляется управлением только в случаях:

-наличия согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством РФ;

-наличия заключенного договора, по которому управление обязуется осуществлять обработку персональных данных субъектов по поручению оператора;

-необходимости достижения целей, предусмотренных нормативно-правовыми актами Российской Федерации и трудовым законодательством, для осуществления и выполнения возложенных законодательством РФ на управление функций, полномочий и обязанностей;

-необходимости осуществления прав и законных интересов управления или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

-когда персональные данные открыты для неограниченного круга лиц, доступ к которым предоставлен субъектом персональных данных либо по его просьбе;

-обязательного раскрытия и подлежащих к опубликованию персональных данных в соответствии с законодательством РФ;

-организации пропускного режима на территории управления.

2.3.Согласно требованиям Федерального закона № 152 от 27.07.2006 «О персональных данных» управление в установленном порядке прошло регистрацию как оператор персональных данных. В открытом и общедоступном реестре операторов персональных данных, размещенном на официальном сайте Роскомнадзора как уполномоченного лица по защите прав и свобод субъектов персональных данных, содержится следующая актуальная информация:

-адрес управления;

-цели обработки персональных данных;

-категории персональных данных;

-категории субъектов, персональные данные которых обрабатываются;

- правовое основание обработки персональных данных;

-перечень действий с персональными данными, общее описание используемых управлением способов обработки персональных данных;

-фамилия, имя, отчество физического лица, ответственного в упарвлении за организацию обработки персональных данных, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;

-описание мер, которые управление обязуется осуществлять при обработке персональных данных по обеспечению безопасности персональных данных при их обработке;

-дата начала обработки персональных данных;

- срок или условие прекращения обработки персональных данных;

-сведения о наличии трансграничной передачи персональных данных в процессе их обработки.

2.4.Управление обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ и договором с субъектом.

2.5.Управление не обрабатывает специальные и биометрические категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведения, характеризующие биологические и физические особенности человека.

2.6.Управление не осуществляет трансграничную передачу персональных данных субъектов персональных данных.

2.7.Управление не принимает решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

3.Меры, направленные на обеспечение выполнения обязанностей, предусмотренных законодательством РФ

3.1.Управление осуществляет следующие организационно-технические меры для защиты персональных данных:

-назначение лица, ответственного за организацию обработки персональных данных;

-издание документов, определяющих политику управления в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

-применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152 «О персональных данных», включая:

а)определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных управления;

б)применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

в)применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

г)оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных управления;

д)учет машинных носителей персональных данных;

е)обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

ж)восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з)установление правил доступа к персональным данным, обрабатываемых в информационных системах персональных данных управления, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных управления;

и)контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных управления.

-осуществление внутреннего контроля соответствия обработки персональных данных законодательству РФ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике управления в отношении обработки персональных данных, локальным актам управления;

-оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства РФ, соотношение указанного вреда и принимаемых в управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством РФ;

-ознакомление сотрудников управления, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику управления в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

-доступ к содержанию электронного журнала сообщений возможен исключительно для администратора безопасности.

4.Права субъекта персональных данных на доступ к его персональным данным

4.1.Субъект персональных данных имеет право на получение сведений, указанных в п.4.6 настоящего раздела, за исключением случаев, предусмотренных законодательством РФ. Субъект персональных данных вправе требовать от представителей управления уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.2.Сведения, указанные в п.4.6 настоящего раздела, предоставляются представителями управления субъекту персональных данных в доступной форме.

4.3.Сведения, указанные в п.4.6 настоящего раздела, предоставляются субъекту персональных данных или его представителю представителями управления при получении запроса субъекта персональных данных или его представителя в письменной форме.

4.4.В случае, если сведения, указанные в п.4.6 настоящего раздела, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к представителям управления или направить в управление повторный запрос в письменной форме в целях получения сведений, указанных в п.4.6 настоящего раздела, и ознакомления с такими персональными

данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

4.5.Субъект персональных данных вправе обратиться повторно к представителю управления или направить повторный письменный запрос в управление в целях получения сведений, указанных в п.4.6 настоящего раздела, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п.4.4 настоящего раздела, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

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

1) подтверждение факта обработки персональных данных управления;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые управлением способы обработки персональных данных;

4) наименование и место нахождения управления, сведения о лицах (за исключением сотрудников управления), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с управлением или на основании законодательства РФ;

5)обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

7)порядок осуществления субъектом персональных данных прав, предусмотренных законодательством РФ;

8)информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9)наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению управления, если обработка поручена или будет поручена такому лицу.

5.Правила работы с обезличенными персональными данными

5.1.Правила работы с обезличенными персональными данными управления разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

5.2.Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных управления и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.3.Способы обезличивания при условии дальнейшей обработки персональных данных:

5.3.1.уменьшение перечня обрабатываемых сведений;

5.3.2.замена части сведений идентификаторами;

5.3.3.обобщение – понижение точности некоторых сведений;

5.3.4.понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

5.3.5.деление сведений на части и обработка в разных информационных системах;

5.3.6.иные способы обезличивания, предусматривающие возможность дальнейшей обработки данных;

5.4.Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных;

5.5.Для обезличивания персональных данных применяются любые способы, не запрещенные законодательством;

5.6.Перечень должностей государственных гражданских служащих управления, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в п.7 Политики;

5.7.Решение о необходимости обезличивания персональных данных принимает ответственный за организацию обработки персональных данных в управлении;

5.8.Ответственные за эксплуатацию ИСПДн готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, если это необходимо;

5.9.Сотрудники структурных подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за эксплуатацию ИСПДн, осуществляют непосредственное обезличивание выбранным способом.

6. Порядок работы с обезличенными персональными данными

6.1.Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

6.2.При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

6.2.1.парольной политики;

6.2.2.антивирусной политики;

6.2.3.правил работы со съемными носителями (если они используется);

6.2.4.правил резервного копирования;

6.2.5.правил доступа в помещения, где расположены элементы информационных систем;

6.2.6.иных способов, предусмотренных законодательством РФ и правовыми актами.

6.3.При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

6.3.1.правил хранения бумажных носителей;

6.3.2.правил доступа к ним и в помещения, где они хранятся;

6.3.3.иных способов, предусмотренных законодательством РФ и правовыми актами.

7.Перчень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Начальник управления;
2. Заместитель начальника управления, начальник отдела экспертизы;
3. Консультант управления.