



РАСПОРЯЖЕНИЕ
АДМИНИСТРАЦИИ ГОРОДА КОГАЛЫМА
Ханты-Мансийского автономного округа - Югры

От «04» мая 2017 г.

№ 93-р

О защите информации
при обработке персональных данных

В соответствии с Федеральным законом Российской Федерации 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», постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» с целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Когалыма:

1. Утвердить состав комиссии по защите информации согласно приложению 1 к настоящему распоряжению.

2. Утвердить положение о комиссии по защите информации согласно приложению 2 к настоящему распоряжению.

3. Утвердить перечень информационных систем согласно приложению 3 к настоящему распоряжению.

4. Утвердить перечень обрабатываемых персональных данных согласно приложению 4 к настоящему распоряжению.

5. Утвердить положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, согласно приложению 5 к настоящему распоряжению.

6. Утвердить политику в отношении обработки персональных данных согласно приложению 6 к настоящему распоряжению.

7. Утвердить инструкции и правила по защите информации:



Приложение 6
к распоряжению Администрации
города Когалыма
от 04.05.2017 №93-р

ПОЛИТИКА в отношении обработки персональных данных

1. Общие положения

1.1. Политика в отношении обработки персональных данных в Администрации города Когалыма (далее – Политика) разработана в соответствии с Конституцией Российской Федерации, Трудовым 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», 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 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», распоряжение ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и другими нормативными правовыми актами, регулирующими отношения, связанные с обработкой персональных данных.

1.2. Политика определяет порядок и условия обработки персональных данных в Администрации города Когалыма (далее - Администрация) с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных осуществляется в следующих целях:

- выполнение требований действующего законодательства Российской Федерации о государственной гражданской службе Российской Федерации и Ханты-Мансийского автономного округа – Югры в части ведения кадрового учета, заключение служебных контрактов, ведение личных дел (карточек), ведение воинского учета, профилактика коррупционных и иных правонарушений;
- оказание государственных и муниципальных услуг по муниципальным контрактам на поставку товаров, выполнение работ, оказание услуг по гражданско-правовым договорам;

- ведение учета сведений о жилом фонде муниципального образования, а также учета граждан, нуждающихся в улучшении жилищных условий;
- администрирование электронного документооборота;
- оказание государственных и муниципальных услуг по внесению в Реестр субъектов потребительского рынка поставщиков товаров, работ и услуг на территории города Когалыма;
- осуществления учета детей, оставшихся без попечения родителей;
- оказания содействия в устройстве детей, оставшихся без попечения родителей, на воспитание в семьи граждан Российской Федерации, постоянно проживающих на территории Российской Федерации;
- создания условий для реализации права граждан, желающих принять детей на воспитание в свои семьи, на получение полной и достоверной информации о детях, оставшихся без попечения родителей;
- оказания содействия гражданам, желающих принять ребенка на воспитание в свою семью;
- ведение информационной базы данных об опекунах, попечителях, приёмных родителях, усыновителях;
- оказание государственных и муниципальных услуг по государственной регистрации актов гражданского состояния;
- оказание государственных и муниципальных услуг для выполнения требований административного законодательства РФ и ХМАО – Югры;
- осуществление учета граждан, желающих принять детей на воспитание в свои семьи;
- реализации трудовых отношений;
- осуществления полномочий по решению вопросов местного значения и отдельных государственных полномочий, переданных органам местного самоуправления федеральными законами, законами Ханты-Мансийского автономного округа - Югры.

1.4. Политика вступает в силу с момента подписания главой города Когалыма.

1.5. Политика подлежит пересмотру в ходе периодического анализа со стороны руководства Администрации, а также в случаях изменения действующего законодательства Российской Федерации в области обеспечения безопасности персональных данных (далее - ПДн).

Политика подлежит опубликованию на официальном сайте Администрации города Когалыма admkogalym.ru в течение 10 дней после её утверждения.

2. Основные понятия

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. 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.

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

2.7. 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.

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

2.9. Информационная система – совокупность содержащихся в базах данных информации и обеспечивающих их обработку информационных технологий и технических средств.

2.10. Государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

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

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Администрацией обеспечивается принятие необходимых мер по удалению или уточнению неполных, или неточных данных.

3.7. Хранение персональных данных 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, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных». Обработка персональных данных допускается в следующих случаях:

4.1.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.1.2. обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию функций, полномочий и обязанностей;

4.1.3. обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

4.1.4. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4.1.5. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.1.6. обработка персональных данных необходима для осуществления прав и законных интересов Администрации или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4.1.7. обработка персональных данных осуществляется в статистических целях, при условии обязательного обезличивания персональных данных;

4.1.8. осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

4.1.9. осуществляется обработка персональных данных, подлежащих опубликованию на официальном сайте Администрации или обязательному раскрытию в соответствии с федеральным законом.

4.2. В случае, если Администрация поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Администрация. Лицо, осуществляющее обработку персональных данных по поручению Администрации, несет ответственность перед Администрацией.

4.3. В целях информационного обеспечения Администрация может создавать общедоступные источники персональных данных сотрудников, в том числе справочники и адресные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты. Сведения о работнике должны быть в любое время исключены из общедоступных источников персональных данных по требованию сотрудника либо по решению суда или иных уполномоченных государственных органов.

5. Конфиденциальность персональных данных

5.1. Сотрудники Администрации, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. Право субъекта персональных данных на доступ к его персональным данным

6.1. Субъект персональных данных имеет право на получение сведений, указанных в пункте 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Администрации 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.

6.2. Сведения, указанные в пункте 6.7 настоящей Политики, должны быть предоставлены субъекту персональных данных Администрацией в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных

6.3. Сведения, указанные в пункте 6.7 настоящей политики, предоставляются субъекту персональных данных или его представителю Администрацией при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Администрацией, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.4. В случае, если сведения, указанные в пункте 6.7 настоящей Политики, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Администрации или направить ему повторный запрос в целях получения сведений, указанных в пункте 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.5. Субъект персональных данных вправе обратиться повторно к Администрации или направить ему запрос в целях получения сведений, указанных в пункте 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемы персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 6.3 настоящей Политики, должен содержать основание направления повторного запроса.

6.6. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным пунктом 6.3 и пунктом 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств

обоснованности отказа в выполнении повторного запроса лежит на Администрации.

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

6.7.1. подтверждение факта обработки персональных данных Администрацией;

6.7.2. правовые основания и цели обработки персональных данных;

6.7.3. цели и применяемые Администрацией способы обработки персональных данных;

6.7.4. наименование и место нахождения Администрации, сведения о лицах (за исключением сотрудников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании федерального закона;

6.7.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

6.7.6. сроки обработки персональных данных, в том числе сроки их хранения;

6.7.7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

6.7.8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.7.9. наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такому лицу;

6.7.10. иные сведения, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

6.8. Право на обжалование действий или бездействий Администрации

6.8.1. Если субъект персональных данных считает, что Администрация осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Администрации в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке.

6.8.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Обязанности Администрации при сборе персональных данных

7.1. При сборе персональных данных Администрация обязана предоставить субъекту персональных данных по его просьбе информацию, предусмотренную пункте 6.7 настоящей Политики.

7.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Администрация обязана разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

7.3. Если персональные данные получены не от субъекта персональных данных, Администрация, за исключением случаев, предусмотренных пунктом 7.4 настоящей Политики, до начала обработки таких персональных данных обязана предоставить субъекту персональных данных следующую информацию:

7.3.1. наименование либо фамилия, имя, отчество и адрес Администрации или его представителя;

7.3.2. цель обработки персональных данных и ее правовое основание;

7.3.3. предполагаемые пользователи персональных данных;

7.3.4. установленные настоящим Федеральным законом права субъекта персональных данных;

7.3.5. источник получения персональных данных.

7.4. Администрация освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 7.3 настоящей Политики, в случаях, если:

7.4.1. субъект персональных данных уведомлен об осуществлении обработки его персональных данных Администрацией;

7.4.2. персональные данные получены Администрацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

7.4.3. персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

7.4.4. предоставление субъекту персональных данных сведений, предусмотренных частью 7.3 настоящей Политики, нарушает права и законные интересы третьих лиц.

8. Меры, направленные на обеспечение выполнения Администрации обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»

8.1. Назначение ответственного за организацию обработки персональных данных.

8.2. Издание документов, определяющие политику Администрации в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

8.3. Утверждение правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.

8.4. Провести ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе, документами, определяющими политику Администрации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

9. Меры по обеспечению безопасности персональных данных при их обработке

9.1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

9.2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.

9.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

9.4. Ведется учет машинных носителей персональных данных.

9.5. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

9.6. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.7. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

9.8. При передаче (подготовке к передаче) персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны, защита от раскрытия, модификации или навязывания (ввода ложной информации) осуществляется путем применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

9.9. Для исключения несанкционированного просмотра персональных данных на устройствах вывода (отображения, печати) информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны, их не размещают напротив оконных проемов, входных дверей, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

9.10. Осуществляется выявление, анализ и устранение уязвимостей информационных систем персональных данных на этапах создания и эксплуатации информационных систем персональных данных. Такие проверки проводятся с периодичностью один раз в месяц, с учетом того, что

должны быть проведены обязательные проверки для критических уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации (далее –ЗИ), технических средств (далее – ТС) и программного обеспечения (далее – ПО), применяемом в информационных системах персональных данных. При выявлении уязвимости составляется отчет и разрабатывается план по их устранению.

9.11. Осуществляется непрерывный контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности персональных данных.