

АДМИНИСТРАЦИЯ ГОРОДА КОТОВСКА
ТАМБОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

21.11.2013

г. Котовск

№ 2912

Об организации обработки персональных данных в администрации города

В целях совершенствования работы по организации обработки персональных данных в администрации города, в соответствии с 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»:

1. Утвердить Правила обработки персональных данных в администрации города согласно приложению №1.

2. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей согласно приложению №2.

3. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города согласно приложению №3.

4. Утвердить Правила работы с обезличенными персональными данными в администрации города согласно приложению №4.

5. Утвердить перечень информационных систем персональных данных администрации города согласно приложению №5.

6. Утвердить перечень персональных данных, обрабатываемых в администрации города в связи с реализацией трудовых отношений, оказанием муниципальных услуг или иных муниципальных функций согласно приложению №6.

7. Утвердить типовую должностную инструкцию ответственного за организацию обработки персональных данных в администрации города согласно приложению №7.

8. Утвердить типовое обязательство работника администрации города, замещающего должность, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора

прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, согласно приложению №8.

9. Утвердить типовую форму согласия на обработку персональных данных согласно приложению №9.

10. Утвердить типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно приложению №10.

11. Утвердить Порядок доступа работников в помещения администрации города, в которых ведется обработка персональных данных, согласно приложению №11.

12. Организационному отделу администрации города направить настоящее постановление для размещения на сайте www.top68.ru в информационно-коммуникационной сети «Интернет».

13. Муниципальному казенному учреждению «Информационно-аналитический центр» (Буханова) разместить настоящее постановление на официальном сайте администрации города в информационно-телекоммуникационной сети «Интернет».

13. Контроль за исполнением настоящего постановления возложить на управляющего делами администрации города А.В. Плаксина.

Первый заместитель главы
администрации города

Л.В. Хлусова

Приложение №1
УТВЕРЖДЕНЫ
постановлением администрации города
от 21.11.2013 № 2912

ПРАВИЛА
обработки персональных данных в администрации города

1. Общие положения

Настоящие Правила обработки персональных данных в администрации города (далее - Правила) направлены на предотвращение нарушений законодательства Российской Федерации, регулирующего обработку персональных данных (далее - ПДн), а также определяющие содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей обработки ПДн.

Правила разработаны в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, 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», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, нормативными и методическими документами по технической защите информации Гостехкомиссии России, ФСТЭК России и ФСБ России, постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Категории субъектов ПДн

В администрации города осуществляется обработка ПДн следующих субъектов ПДн:

- муниципальных служащих;
- работников, занимающих должности, не отнесенные к должностям муниципальной службы;
- кандидатов, участвующих в конкурсе на замещение вакантных должностей муниципальной службы, на включение в кадровый резерв;
- граждан, включенных в кадровый резерв муниципальной службы;

граждан, направляющих обращения в администрацию города;
награждаемых юридических и физических лиц;
сведения о юридических и физических лицах, поступающие в рамках межведомственного взаимодействия;
кандидатов в присяжные заседатели федеральных судов общей юрисдикции Российской Федерации;
избирателей, участников референдумов по городу;
руководителей организаций и учреждений;
собственников и арендаторов земельных участков;
собственников рекламных конструкций.

3. Принципы обработки ПДн

Обработка ПДн должна осуществляться на законной и справедливой основе.

Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

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

Обработке подлежат только ПДн, которые отвечают целям их обработки.

Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Должны приниматься необходимые меры по удалению или уточнению неполных или неточных данных.

Хранение ПДн должно осуществляться в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом или иным нормативно-правовым актом. 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. Цели обработки ПДн

Цели обработки ПДн должны быть четко определены и соответствовать: заявленным в Уставе города, положениях о структурных подразделениях администрации города основным полномочиям и правам;

задачам и функциям администрации города и структурных подразделений администрации города (должностных лиц), указанным в соответствующих положениях, регламентах, должностных инструкциях.

Цели обработки ПДн определяют:
содержание и объем обрабатываемых ПДн;
категории субъектов, ПДн;
сроки их обработки и хранения;
порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Цели обработки ПДн должны быть:
конкретны;
заранее определены;
законны;
заявлены.

Обработка ПДн в администрации города осуществляется для исполнения наделенных полномочий, организации кадровой работы, финансовой деятельности в соответствии с действующим Уставом, положениями, регламентами.

5. Способы и правила обработки ПДн

5.1. В администрации города применяется два способа обработки ПДн:
обработка ПДн без использования средств автоматизации;
обработка ПДн с использованием средств автоматизации.

5.2. Правила обработки ПДн без использования средств автоматизации.

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели, обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации;

имя (наименование) и адрес оператора;
фамилию, имя, отчество и адрес субъекта ПДн;
источник получения ПДн;

сроки обработки ПДн;

перечень действий с ПДн, которые будут совершаться в процессе их обработки;

общее описание используемых оператором способов обработки ПДн;

типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку ПДн;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели, обработки которых заведомо не совместимы.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению отдельной обработки ПДн, в частности:

при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн; при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными ПДн.

5.3. Правила обработки ПДн с использованием средств автоматизации.

Обработка ПДн с использованием средств автоматизации допускается в следующих случаях:

обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

обработка ПДн необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных на администрацию города функций, полномочий и обязанностей; обработка ПДн необходима для ис-

полнения договора, стороной которого является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн;

обработка ПДн необходима для предоставления муниципальных услуг гражданам и организациям;

обработка ПДн необходима для осуществления прав и законных интересов администрации города или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;

осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (ПДн, сделанные общедоступными субъектом ПДн);

осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка ПДн средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные, определенных для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящих Правил.

6. Обработка ПДн с согласия субъекта ПДн

Оператор перед обработкой ПДн получает у субъектов обработки ПДн согласие на обработку ПДн.

Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем только в письменной форме. равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с действующим законодательством электронной подписью.

Получение согласия субъекта ПДн в форме электронного документа на обработку его ПДн в целях предоставления муниципальных услуг, осуществляется в порядке, установленном Правительством Российской Федерации.

В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются оператором.

Допускается включение согласия в типовые формы (бланки) материальных носителей ПДн и в договор с субъектом ПДн.

Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления запроса в администрацию города.

7. Обработка ПДн без согласия субъекта ПДн

Обработка ПДн без получения согласия на такую обработку от субъекта ПДн может осуществляться при наличии оснований, предусмотренных пунктами 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

8. Правила обработки ПДн при поручении обработки ПДн другому лицу

Администрация города вправе поручить обработку ПДн другому лицу (поручение оператора):

- с согласия субъекта ПДн;
- если иное не предусмотрено федеральным законом;
- на основании заключаемого с этим лицом договора, в том числе муниципального контракта;
- путем принятия соответствующего акта.

Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн.

В случае, если администрация города поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет администрация города.

В случае необходимости получения согласия на обработку ПДн от субъекта ПДн обязанность получения такого согласия возлагается на администрацию города.

9. Правила обработки ПДн в зависимости от категории обрабатываемых ПДн

9.1. В администрации города устанавливаются следующие особые правила обработки ПДн в зависимости от категории обрабатываемых ПДн:

- обработка специальных категорий ПДн;
- обработка биометрических ПДн;
- обработка общедоступных ПДн.

9.2. Правила обработки специальных категорий ПДн

К специальным категориям ПДн относятся сведения, касающиеся:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- состояния здоровья;
- интимной жизни;
- судимости.

В администрации города разрешается обработка сведений специальных категорий ПДн при обязательном соблюдении любого из следующих условий:

субъект ПДн дал согласие в письменной форме на обработку своих ПДн; обработка ПДн осуществляется в соответствии с законодательством Российской Федерации;

обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц; обработка ПДн о судимости осуществляется в пределах полномочий, предоставленных администрации города в соответствии с законодательством Российской Федерации.

9.3. Правила обработки биометрических ПДн.

К биометрическим ПДн относятся (обязательное выполнение всех условий одновременно):

сведения, которые характеризуют физиологические и биологические особенности человека;

сведения, на основании которых можно установить его личность.

В случае принятия решения об обработке биометрических ПДн, такие данные могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн.

9.4. Правила обработки общедоступных ПДн.

Общедоступные ПДн физических лиц, полученные из сторонних общедоступных источников ПДн, обрабатываются в исключительных случаях в сроки, не превышающие необходимые для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта ПДн на включение такой информации в общедоступные источники ПДн, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на администрацию города.

По достижении целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия со сторонними физическими и юридическими лицами в администрации города могут создаваться общедоступные источники ПДн. Создание общедоступного источника ПДн осуществляется по решению главы администрации города. В решении о создании общедоступного источника ПДн должны быть указаны:

цель создания общедоступного источника ПДн;

ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника ПДн (при наличии);

перечень ПДн, которые вносятся в общедоступный источник ПДн;

порядок включения ПДн в общедоступный источник ПДн;

порядок уведомления пользователей общедоступного источника ПДн;

порядок получения письменного согласия субъекта ПДн на включение ПДн в общедоступный источник ПДн.

В общедоступный источник ПДн с письменного согласия субъекта ПДн могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники ПДн субъекта ПДн допускается только на основании его письменного согласия.

Исключение ПДн из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта ПДн в соответствии с действующим законодательством Российской Федерации.

10. Правовое основание обработки ПДн

10.1. Правовое основание обработки ПДн включает в себя: определение законности целей обработки ПДн;

оценку вреда, который может быть причинен субъекту ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн;

определение заданных характеристик безопасности ПДн;

определение сроков обработки, в том числе хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

10.2. Определение законности целей обработки ПДн.

Заявляемые цели обработки ПДн должны быть законны, причем, должны рассматриваться и соответственно иметь правовое основание особые правила обработки ПДн (таких как специальные категории ПДн, биометрические ПДн и др.).

При определении правовых оснований обработки ПДн должны определяться реквизиты федеральных законов, а также иных подзаконных актов и документов, которые требуют обработки ПДн или иных документов, являющихся такими основаниями.

Обработка ПДн без документально определенного и оформленного правового основания обработки ПДн не допускается.

10.3. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Оценкой вреда, который может быть причинен субъекту ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта ПДн, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающих его права, свободы и законные интересы.

При обработке ПДн должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта ПДн, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

Обработка ПДн без оценки вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, не допускается.

10.4. Заданные характеристики безопасности ПДн.

Всеми лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность ПДн это обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

Вне зависимости от необходимости обеспечения конфиденциальности ПДн, при обработке ПДн должно определяться наличие требований по обеспечению иных характеристик безопасности ПДн, отличных от нее.

К таким характеристикам относятся: требование по обеспечению защищенности от уничтожения ПДн; требование по обеспечению защищенности от изменения ПДн;

требование по обеспечению защищенности от блокирования ПДн;

требование по обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности ПДн устанавливается федеральными законами и иными нормативными правовыми актами.

При определении правовым актом администрации города необходимости обеспечения характеристик безопасности ПДн, отличных от конфиденциальности, основным критерием должна служить оценка вреда, который может быть причинен субъекту ПДн, с чьим ПДн произошло нарушение таких характеристик безопасности.

Обработка ПДн без документально определенного и оформленного решения по определению характеристик безопасности ПДн не допускается.

10.5. Определение сроков обработки, в том числе хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

На основании определенных целей обработки ПДн, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки ПДн, в том числе хранения.

Определение сроков хранения осуществляется в соответствии с требованиями законодательства Российской Федерации, в том числе в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих ПДн, в различных целях, определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку, предусмотренному федеральным законом. При этом в случае наличия ПДн в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных.

Включение в состав Архивного фонда Российской Федерации документов, содержащих ПДн, осуществляется на основании экспертизы ценности документов и оформляется договором между администрацией города и государственным архивом. При этом объем передаваемых документов и условия передачи определяются условиями такого договора и действующими требованиями законодательства об архивном деле Российской Федерации.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящих Правил не распространяется.

Обработка ПДн без документально определенных и оформленных сроков обработки, в том числе хранения ПДн, не допускается.

С целью выполнения требования по уничтожению либо обезличиванию ПДн по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, в администрации города создается комиссия, определяющая факт достижения целей обработки ПДн и достижение предельных сроков хранения документов, содержащих ПДн.

11. Действия (операции) с ПДн

Обработкой ПДн называется любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств ПДн, включая:

- сбор ПДн;
- запись ПДн;
- систематизацию ПДн;
- накопление ПДн;
- хранение ПДн;
- уточнение ПДн;
- извлечение ПДн;
- использование ПДн;
- передачу ПДн;
- обезличивание ПДн;
- блокирование ПДн;

удаление ПДн;
уничтожение ПДн.

Обработка ПДн без определенных и документально оформленных действий (операций), совершаемых с ПДн, не допускается.

12. Осуществление сбора ПДн

12.1. Способы сбора ПДн и источники их получения.

В администрации города применяются следующие способы получения ПДн субъектов ПДн:

заполнение субъектом ПДн соответствующих форм;

получение ПДн от третьих лиц;

получение данных на основании запроса третьим лицам; сбор данных из общедоступных источников.

Получение ПДн допускается только:

непосредственно от субъекта ПДн;

из общедоступных источников;

от третьих лиц.

Получение ПДн из иных источников не допускается.

12.2. Правила сбора ПДн.

Если предоставление ПДн является обязательным в соответствии с федеральными законами, иными нормативно-правовыми документами, оператор ПДн обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

Если основания на обработку ПДн без согласия отсутствуют, то необходимо получение согласия субъекта ПДн на обработку его ПДн. Обработка ПДн без получения такого согласия запрещается.

Если ПДн получены не от субъекта ПДн, оператор до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

наименование оператора или его представителя; сведения о цели обработки ПДн и ее правовое основание; сведения о предполагаемых пользователях ПДн;

сведения об установленных правах субъекта ПДн; сведения об источниках получения ПДн.

Администрация города освобождается от обязанности предоставлять субъекту ПДн сведения в случаях, если:

субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;

ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

Администрация города осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн; предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

13. Осуществление систематизации, накопления, уточнения и использования ПДн

Систематизация, накопление, уточнение, использование ПДн могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки ПДн.

Уточнение ПДн должно производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении ПДн субъекта ПДн принимается лицом, ответственным за организацию обработки ПДн.

Использование ПДн должно осуществляться исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях не допускается.

14. Осуществление передачи ПДн

Передача ПДн в администрации города должна осуществляться с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В администрации города приняты следующие способы передачи ПДн субъектов ПДн:

передача ПДн на электронных и бумажных носителях информации нарочно;

передача ПДн на электронных и бумажных носителях посредством почтовой связи;

передача ПДн по электронным каналам.

Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта ПДн на обработку ПДн или наличие иных законных оснований.

Передача ПДн должна осуществляться на основании: договора с третьей стороной, которой осуществляется передача ПДн; запроса, полученного от третьей стороны, которой осуществляется передача ПДн; исполнения возложенных законодательством Российской Федерации на администрацию города функций, полномочий и обязанностей.

15. Осуществление хранения ПДн

Хранение ПДн в администрации города допускается только в форме документов - зафиксированной на материальном носителе информации (содержащей ПДн) с реквизитами, позволяющими ее идентифицировать и определить субъекта ПДн. При этом предусматриваются следующие виды документов:

изобразительный документ - документ, содержащий информацию, выраженную посредством изображения какого-либо объекта;

фотодокумент - изобразительный документ, созданный фотографическим способом;

текстовый документ - документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

письменный документ - текстовый документ, информация которого зафиксирована любым типом письма;

рукописный документ - письменный документ, при создании которого знаки письма наносят от руки; машинописный документ - письменный документ, при создании которого знаки письма наносят техническими средствами;

документ на машинном носителе - документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, иным нормативным документом.

Хранение ПДн осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного:

доступа к ним;

их уничтожения; изменения;

блокирования;

копирования;

предоставления;

распространения.

16. Осуществление блокирования ПДн

Блокированием ПДн называется временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Блокирование ПДн конкретного субъекта ПДн должно осуществляться во всех информационных системах ПДн, включая архивы баз данных, содержащих такие ПДн.

Блокирование ПДн осуществляется: в случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по

защите прав субъектов ПДн с момента такого обращения или получения указанного запроса на период проверки; в случае отсутствия возможности уничтожения ПДн в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки ПДн оператор ПДн осуществляет снятие блокирования ПДн.

Решение о блокировании и снятии блокирования ПДн субъекта ПДн принимается ответственным за организацию обработки ПДн.

17. Осуществление обезличивания ПДн

Обезличивание ПДн при обработке ПДн с использованием средств автоматизации осуществляется на основании нормативных правовых актов, правил, инструкций, руководств, регламентов и иных документов для достижения заранее определенных и заявленных целей.

Допускается обезличивание ПДн при обработке ПДн без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

18. Осуществление уничтожения ПДн

Уничтожение ПДн - это действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Уничтожение ПДн производится только в следующих случаях:

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;

ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки; в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно; в случае достижения цели обработки ПДн;

в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

При уничтожении ПДн необходимо:

убедиться в необходимости уничтожения ПДн;

убедиться в том, что уничтожаются те ПДн, которые предназначены для уничтожения;

уничтожить ПДн подходящим способом в соответствии с настоящими Правилами или способом, указанным в соответствующем требовании или распорядительном документе;

проверить необходимость уведомления об уничтожении ПДн;

при необходимости уведомить об уничтожении ПДн требуемых лиц.

При уничтожении ПДн применяются следующие способы:

измельчение в бумагорезательной (бумагоуничтожительной) машине - для документов, исполненных на бумаге;

тщательное вымарывание (с проверкой тщательности вымарывания) - для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержащем ПДн;

физическое уничтожение частей носителей информации - разрушение или сильная деформация - для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); CD (DVD)дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

стирание с помощью сертифицированных средств уничтожения информации - для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении ПДн необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части ПДн допускается уничтожать материальный носитель одним из указанных в настоящих Правилах способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

По факту уничтожения ПДн составляется акт об уничтожении ПДн, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки ПДн, присутствовавшим при уничтожении, и утверждается главой администрации города (заместителем главы администрации города).

Хранение актов об уничтожении ПДн осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

19. Права и обязанности субъекта ПДн и администрации города при обработке ПДн

19.1. Права субъекта ПДн

Субъект ПДн, чьи ПДн обрабатываются в администрации города, имеет право:

на получение сведений о подтверждении факта обработки ПДн администрацией города;

на получение сведений о правовых основаниях и целях обработки ПДн;

на получение сведений о лицах (за исключением сведений о муниципальных служащих администрации города), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора или на основании федерального закона;

на получение сведений об обрабатываемых ПДн, относящихся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом; на получение сведений о сроках обработки ПДн, в том числе сроках их хранения;

на получение сведений о порядке осуществления субъектом ПДн своих прав, предусмотренных законодательством в области ПДн;

на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;

на получение сведений о наименовании и адресе лица, осуществляющего обработку ПДн по поручению администрации города, если обработка поручена или будет поручена такому лицу;

на получение иных сведений, предусмотренных законодательством в области ПДн и другими федеральными законами; требовать от администрации города уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

принимать предусмотренные законом меры по защите своих прав;

требовать от администрации города предоставления ему ПДн в доступной форме;

повторного обращения и запроса в целях получения сведений и ознакомления с его ПДн;

заявить возражение против принятия решения на обработку ПДн, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы;

обжаловать действия или бездействие администрации города в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке, если субъект ПДн считает, что администрация города осуществляет обработку его ПДн с нарушением требований федерального закона или иным образом нарушает его права и свободы;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

требовать предоставления безвозмездно субъекту ПДн или его представителю возможности ознакомления с ПДн, относящимися к этому субъекту ПДн;

принимать решение о предоставлении его ПДн и давать согласие на их обработку свободно, своей волей и в своем интересе; отзываться согласие на обработку ПДн.

Кроме указанных прав в вопросах обработки его ПДн субъект ПДн обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

19.2. Обязанности субъекта ПДн.

Субъект ПДн, чьи ПДн обрабатываются в администрации города, обязан:

предоставлять свои ПДн в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом ПДн своих ПДн;

с целью соблюдения его законных прав и интересов подавать только достоверные ПДн.

Кроме указанных обязанностей в вопросах обработки его ПДн на субъекта ПДн налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

19.3. Права администрации города при обработке ПДн субъектов ПДн.

Администрация города при обработке ПДн субъектов ПДн имеет право: обрабатывать ПДн в соответствии с действующим законодательством Российской Федерации;

поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе муниципального контракта, либо путем принятия соответствующего акта;

мотивированно отказать субъекту ПДн в выполнении повторного запроса в целях получения сведений, касающихся обработки его ПДн, при нарушении субъектом ПДн своих обязанностей по подаче такого запроса;

ограничить право субъекта ПДн на доступ к его ПДн в соответствии с федеральными законами, в том числе, если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

ограничить право субъекта ПДн на доступ к его ПДн в соответствии с федеральными законами, в том числе, если доступ субъекта ПДн к его персональным данным нарушает права и законные интересы третьих лиц;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, если иное не предусмотрено федеральными законами; осуществлять или обеспечивать блокирование или уничтожение ПДн, если обеспечить правомерность обработки ПДн невозможно; осуществлять или обеспечивать уничтожение ПДн;

в случае достижения цели обработки ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основании пункта 4 статьи 21 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

в случае отзыва субъектом ПДн согласия на обработку его ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основании пункта 5 статьи 21 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

в случае отсутствия возможности уничтожения ПДн осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами; осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обра-

ботку ПДн, указанных в пункте 2 статьи 22 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

Кроме указанных прав в вопросах обработки ПДн субъектов ПДн администрация города обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

19.4. Обязанности администрации города при обработке ПДн субъектов ПДн.

Администрация города при обработке ПДн субъектов ПДн обязана:

строго соблюдать принципы и правила обработки ПДн;

в случае, если обработка ПДн осуществляется по поручению оператора, строго соблюдать и выполнять требования оператора;

не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников ПДн сведения о субъекте ПДн;

обеспечить конкретность и информированность согласия на обработку ПДн;

получать согласие на обработку ПДн, если иное не предусмотрено действующим законодательством;

в случае получения согласия на обработку ПДн от представителя субъекта ПДн проверять полномочия данного представителя на дачу согласия от имени субъекта ПДн;

представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований обработки ПДн без получения согласия;

строго соблюдать требования к содержанию согласия в письменной форме субъекта ПДн на обработку его ПДн;

немедленно прекратить обработку специальных категорий ПДн, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом;

убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн, до начала осуществления трансграничной передачи ПДн;

предоставить субъекту ПДн сведения по запросу субъекта ПДн в доступной форме, в которых не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;

мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта ПДн;

разъяснить субъекту ПДн порядок принятия решения на обработку его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов;

предоставить субъекту ПДн по его просьбе информацию, касающуюся обработки его ПДн;

разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн, если предоставление ПДн является обязательным в соответствии с федеральным законом; до начала обработки ПДн, полученных не от субъекта ПДн,

предоставить субъекту ПДн информацию о своем наименовании и адресе, цели обработки ПДн и ее правовом основании, предполагаемых пользователях ПДн, об установленных правах субъекта ПДн, источнике получения ПДн;

принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области ПДн, если иное не предусмотрено федеральными законами;

опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн; по запросу уполномоченного органа по защите прав субъектов ПДн представить документы и локальные акты, определяющие политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн;

принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн; сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо при получении запроса субъекта ПДн или его представителя;

в случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя дать в письменной форме мотивированный ответ;

предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн; внести в ПДн необходимые изменения или уничтожить такие ПДн в случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными;

строго соблюдать сроки по уведомлениям, блокированию и уничтожению ПДн;

уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы;

сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию;

в случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;

в случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн оператор обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц; уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и снять блокирование ПДн в случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов;

прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора в случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора; уничтожить ПДн или обеспечить их уничтожение в случае, если обеспечить правомерность обработки ПДн невозможно;

уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган об устранении допущенных нарушений или об уничтожении ПДн;

прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора):

в случае достижения цели обработки ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом;

в случае отзыва субъектом ПДн согласия на обработку его ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных федеральным законом;

уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн;

уведомить уполномоченный орган по защите прав субъектов ПДн в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку ПДн;

назначить лицо, ответственное за организацию обработки ПДн;

предоставлять лицу, ответственному за организацию обработки ПДн, необходимые сведения;

неукоснительно соблюдать все требования настоящих Правил;

ознакомить работников администрации города, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и организовать обучение таких работников.

Кроме указанных обязанностей в вопросах обработки ПДн субъектов ПДн на администрацию города налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

20. Процедуры, направленные на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий

К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий, относятся:

реализация мер, направленных на обеспечение выполнения оператором своих обязанностей;

выполнение предусмотренных законодательством о ПДн обязанностей, возложенных на администрацию города;

обеспечение личной ответственности работников администрации города, осуществляющих обработку либо доступ к персональным данным; организация рассмотрения запросов субъектов ПДн или их представителей и ответов на такие запросы;

организация внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в области ПДн и локальными актами администрации города;

определение порядка доступа работников в помещения, в которых ведется обработка ПДн;

проведение необходимых мероприятий по обеспечению безопасности ПДн и носителей их содержащих;

проведение периодических проверок условий обработки ПДн; повышение осведомленности работников, занимающих должности которые предусматривают обработку ПДн либо доступ к ПДн, путем их ознакомления с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными актами администрации города по вопросам обработки ПДн и организация обучения указанных служащих;

блокирование, внесение изменений и уничтожение ПДн в предусмотренных действующим законодательством в области ПДн случаях;
оповещение субъектов ПДн в предусмотренных действующим законодательством в области ПДн случаях;
разъяснение прав субъекту ПДн в вопросах обработки и обеспечения безопасности их ПДн;
оказание содействия правоохранительным органам в случаях нарушений законодательства в отношении обработки ПДн;
публикация на официальном сайте администрации города в информационно-коммуникационной сети «Интернет» документов, определяющих политику в отношении обработки ПДн.

21. Требования к работникам администрации города, осуществляющим доступ к ПДн или их обработку

Администрация города осуществляет ознакомление работников, непосредственно осуществляющих обработку ПДн или доступ к ним, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), локальными актами администрации города по вопросам обработки ПДн, включая настоящие Правила:

при оформлении трудового договора; при первоначальном допуске к обработке ПДн;

при назначении на должность, связанную с обработкой ПДн или доступом к ним;

после внесения изменений в действующее законодательство Российской Федерации о ПДн, локальные акты администрации города по вопросам обработки ПДн.

Работники администрации города, непосредственно осуществляющие обработку ПДн или доступ к ним, обязаны:

неукоснительно следовать принципам обработки ПДн;

знать и строго соблюдать положения действующего законодательства Российской Федерации в области ПДн;

знать и строго соблюдать положения локальных актов администрации города в области обработки и обеспечения безопасности ПДн;

знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдать конфиденциальность ПДн, не предоставлять третьим лицами не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

не допускать нарушений требований и правил обработки и обеспечения безопасности ПДн;

обо всех подозрениях и ставших известными случаях нарушений требований и правил обработки и обеспечения безопасности ПДн сообщать лицу, ответственному за обработку ПДн.

Работники администрации города несут личную ответственность за соблюдение требований действующего законодательства Российской Федерации, настоящих Правил.

22. Обеспечение безопасности ПДн при их обработке

22.1. В соответствии с требованиями действующего законодательства в области ПДн при обработке ПДн администрация города обязана принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

22.2. Принципы обеспечения безопасности ПДн при их обработке.

Обеспечение безопасности ПДн в администрации города должно осуществляться на основе следующих принципов:

соблюдение конфиденциальности ПДн;

реализация права на доступ к ПДн лиц, доступ которых к таким данным разрешается в рамках действующего законодательства Российской Федерации и локальными нормативными актами администрации города;

обеспечение защиты информации, содержащей ПДн, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;

своевременное обнаружение фактов несанкционированного доступа к ПДн; недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; постоянный контроль за обеспечением уровня защищенности ПДн;

применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности ПДн.

22.3. Требования к уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн, определяется уровень защищенности ПДн в зависимости от объема обрабатываемых ими ПДн и угроз безопасности жизненно важным интересам личности, общества и государства.

Определение уровня защищенности ПДн проводится на этапе ее создания или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем ПДн).

Результаты определения уровня защищенности ПДн оформляются соответствующим актом установки уровня защищенности ПДн.

22.4. Состав мероприятий по обеспечению безопасности ПДн.

Мероприятия по обеспечению безопасности ПДн должны носить комплексный характер и включать в себя правовые, организационные и технические меры.

22.5. Состав мероприятий по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации.

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключаящие несанкционированный к ним доступ.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

22.6. Состав мероприятий по обеспечению безопасности ПДн при их обработке, осуществляемой с использованием средств автоматизации.

Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах ПДн включают в себя:

определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними; учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

учет лиц, допущенных к работе с ПДн в информационной системе;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

Методами и способами защиты информации от несанкционированного доступа являются:

реализация разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам; ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации; разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей, контроль несанкционированного доступа и действий пользователей;

учет и хранение съемных носителей информации, и их использование, исключаящее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия; использование защищенных каналов связи;

размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;

предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

В информационных системах ПДн, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) основными методами и способами защиты информации от несанкционированного доступа являются:

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы; обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности); защита информации при ее передаче по каналам связи;

использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей; использование средств антивирусной защиты.

Обмен ПДн при их обработке в информационных системах ПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств, в том числе средств криптографической защиты информации.

23. Требования к помещениям, в которых производится обработка ПДн

Размещение оборудования информационных систем ПДн, специального оборудования и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения, в которых располагаются технические средства информационных систем ПДн или хранятся носители ПДн, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

24. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, повлекших нарушения прав субъектов ПДн,

администрация города освобождается от ответственности при наличии доказательств указанных выше обстоятельств.

В случае возникновения обстоятельств непреодолимой силы и нарушения прав субъектов ПДн, связанных с такими обстоятельствами, администрация города принимает все меры для извещения субъекта ПДн.

Управляющий делами
администрации города

А.В. Плаксин

Приложение №2
УТВЕРЖДЕНЫ
постановлением администрации города
от 21.11.2013 № 2912

ПРАВИЛА
рассмотрения запросов субъектов персональных данных
или их представителей

1. Общие положения

Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила) регулируют отношения, возникающие при выполнении администрацией города (далее - Оператор) обязательств согласно требованиям статей 14, 20 и 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон №152-ФЗ).

Положения настоящих Правил распространяются на действия оператора при получении запроса от юридических или физических лиц и их законных представителей (далее – субъект ПДн) и уполномоченного органа по защите прав субъектов персональных данных.

Эти действия направлены на определение порядка учета (регистрации), рассмотрение запросов, а также на подтверждение наличия, ознакомления, уточнения, уничтожения персональных данных (далее-ПДн) или отзыв согласия на обработку ПДн, а также на устранение нарушений законодательства, допущенных при обработке ПДн.

Настоящие Правила разработаны в соответствии с 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» и другими нормативными правовыми актами.

2. Организация и проведение работ Оператором по запросу ПДн

Субъект персональных данных имеет право на получение информации, касающейся обработки его ПДн в соответствии с частью 7 статьи 14 Федерального закона № 152-ФЗ.

Право субъекта персональных данных на доступ к его ПДн может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона № 152-ФЗ.

Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными,

устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, предоставляются субъекту ПДн Оператором при получении запроса от субъекта персональных данных.

Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, должны быть предоставлены субъекту ПДн в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Запрос субъекта ПДн должен содержать номер основного документа, удостоверяющего личность субъекта ПДн, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором, либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись субъекта ПДн. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Рассмотрение запросов является служебной обязанностью должностных лиц Оператора, в чьи обязанности входит обработка ПДн.

Должностные лица Оператора обеспечивают: объективное, всестороннее и своевременное рассмотрения запроса; принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов ПДн; направление письменных ответов по существу запроса.

Все поступившие запросы регистрируются в день их поступления в журнале учета запросов граждан (субъектов персональных данных) по вопросам обработки ПДн.

В случае подачи субъектом ПДн повторного запроса, в целях получения сведений, указанных в части 7 статьи 14 Федерального закона №152-ФЗ, необходимо руководствоваться частями 4 и 5 статьи 14 Федерального закона №152-ФЗ. Повторный запрос наряду со сведениями, указанными выше, должен содержать обоснование направления повторного запроса.

Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ.

Такой отказ должен быть мотивированным.

При рассмотрении запроса Оператором принимаются необходимые законные, обоснованные и мотивированные решения для обеспечения своевременного принятия решения по данному запросу.

Субъекту ПДн в письменной форме в установленный срок сообщается о решениях по запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъясняется также порядок обжалования принятого решения.

Оператор обязан сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при запросе субъекта ПДн либо в течение тридцати дней с даты получения запроса субъекта ПДн.

В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн при получении запроса субъекта ПДн Оператор обязан руководствоваться частью 2 статьи 20 Федерального закона № 152-ФЗ.

Оператор обязан:

предоставить безвозмездно субъекту ПДн возможность ознакомления с ПДн, относящимися к этому субъекту ПДн;

уведомить субъекта ПДн о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

Должностное лицо, назначенное главой администрации города, осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

3. Действия Оператора в ответ на запросы по ПДн

3.1. В случае поступления запроса субъекта ПДн по ПДн необходимо выполнить следующие действия:

при получении запроса субъекта ПДн на наличие ПДн необходимо в течение 30 дней с даты получения запроса (согласно части 1 статьи 20 Федерального закона № 152-ФЗ) подтвердить обработку ПДн в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно части 2 статьи 20 Федерального закона №152-ФЗ) необходимо отправить уведомление об отказе в предоставлении информации о наличии ПДн.

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки ПДн Оператором; правовые основания и цели обработки ПДн; цели и применяемые Оператором способы обработки ПДн;

наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании Федерального закона № 152-ФЗ;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;

- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом №152-ФЗ;
- информацию о осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом №152-ФЗ или другими федеральными законами;
- при получении запроса субъекта ПДн или его представителя на уточнение ПДн необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными (согласно части 3 статьи 20 Федерального закона № 152-ФЗ) и отправить уведомление о внесенных изменениях. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе в осуществлении изменения ПДн;
- при получении запроса субъекта ПДн на уничтожение ПДн необходимо их уничтожить в срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно части 3 статьи 20 Федерального закона № 152-ФЗ), и отправить уведомление об уничтожении. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе в уничтожении ПДн;
- при получении запроса на отзыв согласия субъекта ПДн на обработку ПДн необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва (согласно части 5 статьи 21 Федерального закона №152-ФЗ);

при выявлении недостоверности ПДн при обращении или по запросу субъекта персональных данных необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом ПДн или его представителем, либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, необходимо уточнить ПДн в течение 7 рабочих дней со дня представления таких сведений и снять блокирование ПДн (согласно части 2 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе в изменении ПДн;

при выявлении неправомерных действий с ПДн Оператору по запросу субъекта персональных данных необходимо в срок, не превышающий 3 рабочих дней с даты этого выявления, прекратить неправомерную обработку ПДн (согласно части 3 статьи 21 Федерального закона № 152-ФЗ). В случае, если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн (согласно части 3 статьи 21 Федерального закона № 152-ФЗ), обязан уничтожить такие ПДн.

При достижении целей обработки ПДн Оператор обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн (согласно части 4 статьи 21 Федерального закона № 152-ФЗ), если иное не предусмотрено договором, стороной которого или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн, либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн, если иное не предусмотрено действующим законодательством.

3.2. В случае поступления запроса уполномоченного органа по защите прав субъекта ПДн по ПДн необходимо выполнить следующие действия:

при получении запроса необходимо в течение 30 дней (согласно части 4 статьи 20 Федерального закона № 152-ФЗ) предоставить информацию, необходимую для осуществления деятельности указанного органа;

при выявлении недостоверных ПДн по запросу уполномоченного органа по защите прав субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн, необходимо в течение 7 рабочих дней уточнить ПДн и снять их блокирование (согласно части 2 статьи 21 Федерального закона № 152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения и снять блокирование ПДн;

при выявлении неправомерных действий Оператора с ПДн по запросу уполномоченного органа по защите прав субъекта ПДн необходимо прекратить неправомерную обработку ПДн в срок, не превышающий 3 рабочих дней с

момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Федерального закона №152-ФЗ). В случае невозможности обеспечения правомерности обработки Оператором ПДн в срок, не превышающий 10 рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

4. Ответственность Оператора

ПДн не подлежат разглашению (распространению).

Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению информации ограниченного доступа.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 3
УТВЕРЖДЕНЫ
постановлением администрации города
от 21.11.2013 № 2912

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
администрации города

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города (далее - Правила) разработаны в соответствии с требованиями постановления 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».

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (далее - ПДн) с целью своевременного выявления и предотвращения:

- хищения технических средств и носителей информации;
- утраты информации;
- преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;
- несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;
- утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя:
контроль организации защиты информации;
контроль эффективности защиты информации.

2. Порядок внутреннего контроля за соблюдением требований по
обработке и обеспечению безопасности ПДн

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются не реже одного раза в год в соответствии с утвержденным графиком.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

соблюдения принципов обработки ПДн;
соответствия локальных актов в области ПДн действующему законодательству Российской Федерации;

выполнения работниками требований и правил обработки ПДн в информационных системах персональных данных (далее - ИСПДн);

актуальности информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн;

актуальности перечня должностей должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;

актуальности перечня должностных лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;

соблюдения обязанностей оператора ПДн, предусмотренных действующим законодательством в области ПДн;

порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлению, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных; наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;

актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;

актуальности перечня ИСПДн;

знания и соблюдения работниками положений действующего законодательства Российской Федерации в области ПДн, локальных актов администрации города;

соблюдения работниками конфиденциальности ПДн;

соблюдения муниципальными служащими требований по обеспечению безопасности ПДн;

наличия и актуальности локальных актов, технической и эксплуатационной документации технических и программных средств ИСПДн.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает главе администрации города (заместителю главы администрации города).

При проведении внутреннего контроля на ИСПДн составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте по форме, приведенной в приложении к настоящим Правилам.

3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям производится соответствие оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в администрации города.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн производится экспертное сравнение заявленной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, оформляется в виде отдельного документа, подписывается председателем комиссии и утверждается главой администрации города (заместителем главы администрации города).

Управляющий делами
администрации города

А.В. Плаксин

Приложение
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в администрации города

Протокол № ____

контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте

(наименование структурного подразделения администрации города)

1. Объект контроля:
наименование автоматизированного рабочего места (далее-АРМ);
заводской (инвентарный) номер системного блока персональной электронно-вычислительной машины АРМ;
адрес размещения АРМ.
2. Назначение объекта:
тип информации, обрабатываемой (хранимой) на АРМ;
уровень защищенности персональных данных при их обработке в информационной системе.
3. Контролируемые вопросы:
состояние организации технической защиты информации при обработке (хранении) информации ограниченного доступа;
контроль наличия руководящих документов, инструкций, документации, регламентирующей обработку (хранение) информации ограниченного доступа:
перечня защищаемых ресурсов и уровня их конфиденциальности;
перечня лиц, обслуживающих АРМ;
перечня лиц, имеющих право самостоятельного доступа в помещение с АРМ;
перечня лиц, имеющих право самостоятельного доступа к штатным средствам АРМ и уровень их полномочий; распоряжения о назначении администратора информационной безопасности; данных по уровню подготовки персонала;
инструкции по обеспечению защиты информации, обрабатываемой на АРМ;
перечня программного обеспечения;
описания технологического процесса обработки информации; схемы информационных потоков; технического паспорта;
матрицы доступа субъектов к защищаемым информационным ресурсам;
акта установки системы активного шумления (при наличии);

акта установки системы защиты информации от несанкционированного доступа (далее-СЗИ НСД) (при наличии);
описания системы разграничения доступа и настроек СЗИ НСД;
инструкции администратора безопасности;
инструкции пользователя; инструкции по антивирусному контролю;
распоряжения о допуске служащих;
распоряжения о вводе в эксплуатацию.

Контроль соответствия настройки подсистемы управления доступом, подсистемы регистрации и учета, подсистемы обеспечения целостности требованиям присвоенного класса защищенности от НСД.

В соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением Председателя Гостехкомиссии от 30.03.1992, в настройках подсистемы управления доступом проверяется:

наличие требований к длине и сложности пароля;
ограничение максимального срока действия пароля;
настройки блокировки учетных записей при попытках несанкционированного доступа;
наличие административных прав у пользователей;
выполнение требований мандатного разграничения прав доступа к каталогам, программам, файлам.

В настройках подсистемы регистрации и учета контролируется:
отсутствие критических ошибок и несанкционированных запусков процессов, зарегистрированных в журнале приложений;
отсутствие зарегистрированных критических системных ошибок в системном журнале;
отсутствие зарегистрированных изменений действующих политик безопасности, прав доступа, настроек системы защиты информации в журнале системы защиты информации; возможности несанкционированного доступа к информации, аудиты отказа, зарегистрированные в журнале безопасности.

В настройках подсистемы обеспечения целостности контролируется:
соответствие программного обеспечения, установленного на АРМ, аттестационным материалам; отсутствие программных средств разработки и отладки приложений;

наличие средств антивирусного контроля, включая срок действия лицензии и периодичность обновления антивирусных баз.

Контроль наличия лицензионного программного обеспечения, установленного в процессе проведенной аттестации по требованиям безопасности информации.

Контроль срока действия лицензии, порядка и периодичности обновления баз антивирусной программы.

Контроль наличия сетевых плат (в том числе интегрированных) и физической возможности их использования.

Контроль возможности и фактов подключения незарегистрированных внешних носителей информации.

4. Метод проведения контроля: экспертно-документальный.

5. Средства контроля: программные возможности операционной системы, установленной на контролируемом АРМ.

6. Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации.

Контроль проводится в соответствии с требованиями:

Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

специальных требований и рекомендаций по технической защите конфиденциальной информации (приказ Гостехкомиссии России от 30.08.2002 № 282);

руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (решение Председателя Гостехкомиссии от 30.03.1992);

руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (приказ Председателя Гостехкомиссии России от 04.06.1999 №114);

нормативных и руководящих документов ФСТЭК России по защите информации.

Контроль выполнил:

_____	_____	_____
должность	подпись	фамилия, инициалы

При проведении контроля присутствовали:

_____	_____	_____
должность	подпись	фамилия, инициалы

_____	_____	_____
должность	подпись	фамилия, инициалы

Дата проведения контроля: _____
(число, месяц, год)

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 4
УТВЕРЖДЕНЫ
постановлением администрации города
от 21.11.2013 № 2912

ПРАВИЛА
работы с обезличенными персональными данными
в администрации города

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными в администрации города (далее - Правила) разработаны с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления 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».

2. Условия обезличивания

Обезличивание персональных данных (далее-ПДн) проводится с целью снижения ущерба от разглашения защищаемых ПДн и снижения требований к защите информационной системы персональных данных (далее-ИСПДн).

Обезличивание персональных данных также осуществляется по достижению целей обработки ПДн или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

Способы обезличивания при условии дальнейшей обработки ПДн:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- замена численных значений минимальным, средним или максимальным значением;
- обобщение - понижение точности некоторых сведений;
- деление сведений на части и обработка их в разных информационных системах;
- другие способы.

Для обезличивания ПДн применяются любые способы явно не запрещенные законодательно.

Руководители структурных подразделений администрации города, непосредственно осуществляющих обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и определяют способ обезличивания.

3. Порядок работы с обезличенными персональными данными

Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями;
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 5
УТВЕРЖДЕН
постановлением администрации города
от 21.11.2013 № 2912

Перечень информационных систем персональных данных администрации города

№ п/п	Наименование ИСПДн (её составной части)	Наименование объекта (полное и сокращенное) Отраслевая (ведомственная) принадлежность Адрес объекта	Исходные данные классификации ИСПДн					Класс ИСПДн	Примечание
			Структура ИСПДн (количество серверов/ПЭВМ)	Наличие подключений к ССОП и сетям МИО (Интернет)	Режим обработки ПДн	Разграничение доступа пользователей	Нахождение ИСПДн (её составных частей) в пределах России		
1	2	3	4	5	6	7	8	9	10
1.	1С	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Локальная система 1 Сервер, 3 ПК	Подключена к сети Интернет (используются по необходимости)	Многопользовате льский	С разграничением прав доступа	Расположена в России	3	Автоматизир ованная
2.	Обращения граждан	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Автономная система 1 ПК	Подключение к сети интранет	Однопользовател ьский	Без разграничения	Расположена в России	3	Автоматизир ованная

3.	Аренда земли	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Автономная система 1 ПК	Не имеет подключения	Однопользовател ьский	Без разграничения	Расположена в России	2	Автоматизир ованная
4	Аренда земли	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Автономная система 1 ПК	Не имеет подключения	Однопользовател ьский	Без разграничения	Расположена в России	2	Автоматизир ованная
5	1С	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Локальная система 1 Сервер, 4ПК	Подключена к сети Интернет (используются по необходимости)	Многопользовате льский	С разграничением прав доступа	Расположена в России	3	Автоматизир ованная
6	Учёт граждан, нуждающихся в жилых помещениях.	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	-	-	-	-	Расположена в России	-	Не автоматизиро ванная

7	Учёт граждан, нуждающихся в жилых помещениях и признанных малоимущими	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	-	-	-	-	Расположена в России	-	Не автоматизиро ванная
8	Список молодых семей — участников программы «Молодежи - доступное жилье»	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	-	-	-	-	Расположена в России	-	Не автоматизиро ванная
9	ИС «Шафл-Шлюз»	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Локальная система	Подключение к ИНТРАНЕТ	Многопользовате льский	С ограничением прав доступа	Расположена в России	3	Автоматизир ованная
	ИС «СБИС++ Электронная отчетность»	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	Локальная система	Подключена к сети Интернет (используются по необходимости)	Многопользовательс кий	С ограничением прав доступа	Расположена в России	3	Автоматизир ованная

	«Отдел кадров».	Администрация 393190 Тамбовская область г.Котовск ул Свободы д 8	'	'	'	'	Расположена в России	-	Не автоматизиро ванная
--	-----------------	---	---	---	---	---	-------------------------	---	------------------------------

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 6
УТВЕРЖДЕН
постановлением администрации города
от 21.11.2013 № 2912

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в администрации города в связи с реализацией трудовых отношений, оказанием муниципальных услуг или иных муниципальных функций

1. Биометрические персональные данные.
2. Фамилия, имя, отчество.
3. Пол.
4. Дата рождения.
5. Место рождения.
6. Адрес фактического проживания, адрес прописки.
7. Сведения о членах семьи.
8. Социальное положение.
9. Сведения о доходах, имуществе и обязательствах имущественного характера.
10. Сведения об образовании.
11. Сведения о трудовой деятельности.
12. Сведения о доходах.
13. Паспортные данные.
14. Данные об обязательном пенсионном страховании.
15. Сведения о постановке на налоговый учёт.
16. Сведения о воинском учёте, службе.
17. Сведения о медицинском страховании.
18. Гражданство.
19. Наличие судимости.
20. Сведения о допуске к государственной тайне или иной охраняемой законом информации.
21. Сведения о близких родственниках.
22. Сведения о пребывании за границей.
23. Сведения об участии в выборных представительных органах.
24. Сведения о наградах.
25. Сведения о состоянии здоровья.
26. Номера телефонов (стационарных, мобильных, служебных, личных).
27. Сведения о владении иностранным языком.
28. Сведения о дисквалификации.

Приложение № 7
УТВЕРЖДЕНА
постановлением администрации города
от 21.11.2013 № 2912

ТИПОВАЯ
должностная инструкция ответственного за организацию обработки
персональных данных в администрации города

Ответственным за организацию обработки персональных данных (далее – Ответственный) является штатный сотрудник (наименование органа администрации города), назначенный главой администрации города.

Ответственный в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами администрации города и отвечает за поддержание необходимого уровня безопасности обработки персональных данных (далее - ПДн).

Ответственный осуществляет методическое руководство сотрудниками, имеющими санкционированный доступ к ПДн, в вопросах обеспечения безопасности персональных данных и несет персональную ответственность за качество проводимых им работ по контролю действий сотрудников, имеющих санкционированный доступ к ПДн, состояние и поддержание установленного уровня защиты информационных систем, обрабатывающих ПДн.

Требования ответственного обязательны для исполнения всеми сотрудниками, имеющими санкционированный доступ к ПДн.

Ответственный должен:

знать и соблюдать требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите ПДн;

вести инструктаж сотрудников, имеющих доступ к персональным данным, по организационно-распорядительным документам администрации города;

уточнять в установленном порядке обязанности пользователей объектов защиты;

осуществлять контроль за выполнением плана мероприятий по защите ПДн;

анализировать состояние защиты ПДн;

контролировать исполнение введенного режима безопасности;

не допускать установку, использование, хранение и распространение программных средств, не связанных с выполнением функциональных задач;

не допускать к работе на автоматизированных рабочих местах ПДн посторонних лиц;

в случае отказа работоспособности технических средств и программного обеспечения информационных систем ПДн, в том числе средств защиты, принимать меры по их своевременному восстановлению.

Ответственный имеет право:

подавать руководству прошение о направлении на обучение по защите персональных данных в учебных центрах и на курсах повышения квалификации;

вносить руководству предложения о наказании отдельных сотрудников, имеющих санкционированный доступ к ПДн, допустивших серьезные нарушения в обеспечении безопасности ПДн.

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 8
УТВЕРЖДЕНО
постановлением администрации города
от 21.11.2013 № 2912

Типовое обязательство работника администрации города, замещающего должность, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Обязательство
о соблюдении конфиденциальности персональных данных

Я, _____,
(фамилия, имя, отчество, должность)

непосредственно осуществляя обработку персональных данных при выполнении своих должностных обязанностей, ознакомлен с требованиями по соблюдению конфиденциальности обрабатываемых мною персональных данных субъектов персональных данных и обязуюсь в случае расторжения со мной трудового договора прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я ознакомлен с предусмотренной действующим законодательством Российской Федерации ответственностью за нарушения неприкосновенности частной жизни и установленного порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

(фамилия, имя, отчество)

(паспортные данные)

(подпись)

(дата)

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 9
УТВЕРЖДЕНА
постановлением администрации города
от 21.11.2013 № 2912

ТИПОВАЯ
форма согласия на обработку персональных данных

Я, _____
(Фамилия, имя, отчество субъекта персональных данных)

_____ серия _____ № _____
(вид основного документа, удостоверяющего личность)

выдан _____,
проживающий(ая) по адресу: _____

В лице представителя субъекта персональных данных (заполняется в случае
получения согласия от представителя субъекта персональных данных),

(Фамилия, имя, отчество)

_____ серия _____ № _____
(вид основного документа, удостоверяющего личность)

выдан _____
проживающий(ая) по адресу: _____

действующий от имени субъекта персональных данных на основании

_____ (реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

предоставляю мои персональные данные и даю согласие на их обработку.

Наименование и адрес оператора, получающего согласие субъекта
персональных данных:

Со следующей целью обработки персональных данных:

Перечень персональных данных, на обработку которых дается согласие
субъекта персональных данных: _____

(подпись)

(Ф.И.О.)

Управляющий делами
администрации города

А.В. Плаксин

№Приложение № 10
УТВЕРЖДЕНА
постановлением администрации города
от 21.11.2013 № 2912

ТИПОВАЯ
форма разъяснения субъекту персональных данных юридических последствий
отказа предоставить свои персональные данные
Уважаемый _____!
(Ф.И.О)

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006г. № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

_____ (пункт, статья, часть)
Федерального закона _____,
(реквизиты и наименование)

а также следующими нормативными актами

_____ (указываются реквизиты и наименования таких нормативных актов)
В случае отказа Вами предоставить свои персональные данные Администрация города Тамбова (наименование органа Администрации) не сможет на законных основаниях осуществлять обработку Ваших персональных данных, что приведет к следующим для Вас юридическим последствиям

_____ (перечислить юридические последствия для субъекта персональных данных)
В соответствии с действующим законодательством Российской Федерации в области персональных данных Вы имеете право:
на получение сведений об администрации города как операторе, осуществляющем обработку Ваших персональных данных (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения администрации города (органа администрации), о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от оператора разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;

Продолжение приложения № 10

обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

(ФИО, должность)

(подпись)

(дата)

Управляющий делами
администрации города

А.В. Плаксин

Приложение № 11
УТВЕРЖДЕН
постановлением администрации города
от 21.11.2013 № 2912

ПОРЯДОК
доступа работников в помещения администрации города,
в которых ведется обработка персональных данных

1. Общие положения

Настоящий Порядок доступа работников в помещения администрации города (структурных подразделений администрации города), в которых ведется обработка персональных данных, (далее - Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и 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» и другими нормативными правовыми актами».

Настоящий Порядок регламентирует условия и порядок осуществления доступа работников администрации города и других лиц в помещения администрации города (структурных подразделений администрации города), в которых ведется обработка персональных данных (далее - помещения) в целях обеспечения безопасности персональных данных (далее - ПДн).

Для обеспечения доступа работников администрации города в вышеуказанные помещения предусматривается комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности администрации города (структурных подразделений администрации города).

Указанные меры осуществляются руководителями структурных подразделений администрации города, осуществляющих обработку ПДн.

2. Порядок доступа работников администрации города в помещения

Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн достигается, в том числе, установлением правил доступа в помещения, где ведется обработка ПДн с использованием средств автоматизации или без использования таковых.

Для помещений, в которых обрабатываются ПДн, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ПДн и средств защиты информации, а также исключается возможность

неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

Доступ работников в помещения осуществляется в соответствии со списком работников, имеющих право самостоятельного доступа в помещения, в которых ведется обработка ПДн (далее - Список).

Список утверждается главой администрации города по представлению руководителя структурного подразделения администрации города.

Доступ в помещения иных лиц осуществляется работниками, указанными в Списке. Пребывание посторонних лиц в помещениях допускается только в присутствии вышеуказанных работников.

Управляющий делами
администрации города

А.В. Плаксин