

Утверждено
приказом финансового
управления администрации
Уссурийского городского
округа
от 19.12.2023 года № 8-П

Положение
по обеспечению безопасности персональных данных
в финансовом управлении администрации Уссурийского городского округа

I. Общие положения

1. Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в финансовом управлении администрации Уссурийского городского округа (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон), Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением администрации Уссурийского городского округа от 17 декабря 2013 года № 4261 «Об утверждении Положения по обеспечению безопасности персональных данных в администрации Уссурийского городского округа» и определяет политику

в отношении обработки персональных данных финансового управления администрации Уссурийского городского округа.

2. Настоящее Положение определяет:

а) правовое основание обработки персональных данных в финансовом управлении администрации Уссурийского городского округа (далее – финансовое управление);

б) принципы обработки персональных данных в финансовом управлении;

в) оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона;

г) основные условия проведения обработки персональных данных;

д) правила рассмотрения запросов субъектов персональных данных или их представителей;

е) правила обработки и защиты персональных данных;

ж) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом, принятыми в соответствии с федеральным законом нормативными правовыми актами администрации;

з) соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона, и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом.

3. Настоящее Положение подлежит размещению на официальном сайте администрации Уссурийского городского округа в целях исполнения требования части 2 статьи 18.1 Федерального закона.

4. В настоящем Положении используются термины и определения в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

5. Субъектами персональных данных в финансовом управлении являются:

а) физическое лицо, состоящее с финансовым управлением в отношениях, регулируемых трудовым законодательством, в том числе претендующие на замещение вакантных должностей;

б) физическое лицо, обращающееся к финансовому управлению в связи с осуществлением муниципальных функций.

6. Объектами системы безопасности персональных данных в финансовом управлении являются:

а) информационные ресурсы с ограниченным доступом, содержащие персональные данные;

б) процессы обработки персональных данных в информационной системе персональных данных (далее - ИСПДн) финансового управления, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

в) информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

II. Определение законности целей обработки персональных данных

7. Определение законностей целей обработки персональных данных в финансовом управлении является правовым основанием обработки персональных данных в финансовом управлении.

8. Обработка персональных данных в финансовом управлении осуществляется в целях реализации трудовых отношений, а также в связи осуществлением муниципальных функций возложенных на финансовое управление.

9. Цели обработки персональных данных в финансовом управлении:

а) федеральным законам, а также иным подзаконным актам и документам органов государственной власти, которые требуют обработку персональных данных или иным документам, являющимся такими основаниями;

б) перечням задач или функций, указанным в Положении о финансовом управлении.

10. Цели обработки персональных данных определяют:

а) содержание и объем обрабатываемых персональных данных;

б) категории субъектов, персональные данные которых обрабатываются;

в) сроки их обработки и хранения;

г) порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

III. Принципы обработки персональных данных в финансовом управлении

11. Обработка персональных данных в финансовом управлении осуществляется на основе принципов:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

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

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

д) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;

е) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

ж) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

IV. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных

12. Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения правил обработки и защиты персональных данных.

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

14. При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия

в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения правил обработки и защиты персональных данных при выполнении заявленных в рамках перечня задач или функций органов администрации, указанных в положениях органов администрации с учетом особых правил и способов обработки персональных данных.

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

V. Перечень действий (операций) совершаемых с персональными данными в финансовом управлении

16. Сбор персональных данных.

В финансовом управлении применяются следующие способы получения персональных данных субъектов персональных данных:

- а) заполнение субъектом персональных данных соответствующих форм;
- б) получение персональных данных от третьих лиц;
- в) получение данных на основании запроса по форме согласно Приложению 6 к настоящему Положению;
- г) сбор данных из общедоступных источников.

При сборе персональных данных финансовое управление обязано предоставить субъекту персональных данных по его просьбе информацию, предусмотренную настоящим Положением.

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, финансовое управление обязано

разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные по форме согласно Приложению 3 к настоящему Положению.

Если персональные данные получены не от субъекта персональных данных, финансовое управление до начала обработки таких персональных данных обязано предоставить субъекту персональных данных уведомлении об обработке персональных данных по форме согласно Приложению 9 к настоящему Положению.

При сборе персональных данных финансовое управление обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона.

17. Систематизация, накопление, уточнение и использование персональных данных.

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

В финансовом управлении могут быть установлены особенности учета персональных данных в ИСПДн, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей ИСПДн, конкретному субъекту персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан

или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в ИСПДн, конкретному субъекту персональных данных.

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

При необходимости, уведомить об уточнении персональных данных требуемых лиц в письменном виде по форме согласно Приложению 8 к настоящему Положению.

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

18. Запись и извлечение персональных данных.

Запись персональных данных в ИСПДн финансового управления может осуществляться с любых носителей информации или из других ИСПДн.

Извлечение персональных данных из ИСПДн может осуществляться с целью:

а) вывода персональных данных на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;

б) вывода персональных данных на носители информации, предназначенные для их обработки средствами вычислительной техники.

При извлечении персональных данных должен проводиться учет носителей информации.

При осуществлении записи и извлечения персональных данных должны соблюдаться условия обработки персональных данных, конфиденциальность персональных данных и иные требования, указанные в настоящем Положении.

19. Передача персональных данных.

Передача персональных данных в финансовом управлении должна осуществляться с соблюдением настоящего Положения и действующего законодательства Российской Федерации.

В финансовом управлении приняты следующие способы передачи персональных данных субъектов персональных данных:

- а) передача персональных данных на электронных и бумажных носителях информации нарочным способом;
- б) передача персональных данных на электронных и бумажных носителях посредством почтовой связи;
- в) передача персональных данных по каналам связи.

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

Передача персональных данных должна осуществляться на основании:

- а) договора с третьей стороной, которой осуществляется передача персональных данных;
- б) запроса, полученного от третьей стороны, которой осуществляется передача персональных данных;
- в) исполнения возложенных законодательством Российской Федерации на финансовое управление функций, полномочий и обязанностей.

Передача персональных данных без согласия или иных законных оснований категорически запрещается.

20. Хранение персональных данных.

Хранение персональных данных в финансовом управлении допускается только в форме документов - зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

- а) изобразительный документ - документ, содержащий информацию,

выраженную посредством изображения какого-либо объекта;

б) фотодокумент - изобразительный документ, созданный фотографическим способом;

в) текстовой документ - документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

г) письменный документ - текстовой документ, информация которого зафиксирована любым типом письма;

д) рукописный документ - письменный документ, при создании которого знаки письма наносят от руки;

е) машинописный документ - письменный документ, при создании которого знаки письма наносят техническими средствами;

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

Хранение персональных данных в ИСПДн и вне таких систем финансового управления 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.

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

При использовании документов, содержащих персональные данные, в различных целях определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку.

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящего Положения не распространяется.

Сроки временного хранения документов, включенных в состав Архивного фонда Российской Федерации, до их поступления в муниципальный архив, устанавливаются в соответствии с требованиями архивного законодательства Российской Федерации.

21. Блокирование персональных данных.

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

Блокирование персональных данных конкретного субъекта персональных данных должно осуществляться во всех ИСПДн финансового управления, включая архивы баз данных, содержащих такие персональные данные.

Блокирование персональных данных в финансовом управлении осуществляется:

а) в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя по форме согласно Приложению 12 к настоящему Положению, либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;

б) в случае отсутствия возможности уничтожения персональных данных в установленные сроки до их уничтожения.

При необходимости финансовое управление направляет уведомление о блокировании персональных данных субъектам персональных данных в письменном виде по форме согласно Приложению 7 к настоящему Положению.

После устранения выявленной неправомерной обработки персональных данных финансовое управление осуществляет снятие

блокирования персональных данных. При необходимости финансовое управление направляет уведомление об устранении допущенных нарушений в письменном виде по формам согласно Приложениям 5, 11 к настоящему Положению.

22. Обезличивание персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, установлены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05 сентября 2013 года № 996.

Под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки.

Сотрудники финансового управления, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, осуществляют обезличивание выбранным способом.

23. Уничтожение персональных данных.

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

Уничтожение персональных данных в финансовом управлении производится только в следующих случаях:

а) персональные данные являются незаконно полученными, или не являются необходимыми для заявленной цели обработки;

б) в случае выявления неправомерной обработки персональных данных, если обеспечить правомерность обработки персональных данных невозможно;

в) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных по форме согласно Приложению 15 к настоящему Положению.

При уничтожении персональных данных необходимо:

а) убедиться в необходимости уничтожения персональных данных;

б) убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;

в) уничтожить персональные данные подходящим способом, в соответствии с настоящим Положением или способом, указанным в соответствующем требовании или распорядительном документе;

г) проверить необходимость уведомления об уничтожении персональных данных;

д) при необходимости, уведомить об уничтожении персональных данных требуемых лиц в письменном виде по формам согласно Приложениям 4, 10 к настоящему Положению;

При уничтожении персональных данных применяются следующие способы:

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

б) стирание персональных данных - для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержащем персональные данные;

в) физическое уничтожение (разрушение) носителей информации - для

носителей информации на оптических дисках;

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

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

При уничтожении персональных данных 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 персональных данных допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение персональных данных производится только в присутствии лица, ответственного за организацию обработки персональных данных в финансовом управлении.

По факту уничтожения персональных данных составляется Акт уничтожения персональных данных, который подписывается лицами, производившими уничтожение.

Хранение актов уничтожения персональных данных осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

VI. Права субъектов персональных данных

24. Круг субъектов, персональные данные которых подлежат обработке в ИСПДн финансового управления, определяется целью обработки персональных данных в каждой информационной системе персональных данных.

25. Субъект персональных данных имеет право на получение при обращении информации, касающейся обработки его персональных данных, по формам согласно Приложениям 13, 14, 16 к настоящему Положению, в том числе содержащей следующие сведения:

- а) правовое основания и цель обработки персональных данных;
- б) способы обработки персональных данных;
- в) сведения о лицах (за исключением сотрудников администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с финансовым управлением или на основании федерального закона;
- г) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- д) сроки обработки персональных данных, в том числе сроки их хранения;
- е) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- ж) информацию об осуществленной или о предполагаемой трансграничной передаче данных.

26. Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено в соответствии с федеральным законом в случае, если:

- а) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

в) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

27. Если субъект персональных данных считает, что финансовое управление осуществляет обработку его персональных данных с нарушением требований федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие финансового управления в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

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

29. Финансовое управление освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 25, в случаях, если:

а) субъект персональных данных уведомлен об осуществлении обработки его персональных данных финансовым управлением;

б) персональные данные получены финансовым управлением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

в) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных Федеральным законом;

г) финансовое управление осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом

не нарушаются права и законные интересы субъекта персональных данных;

д) предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

VII. Правила рассмотрения запросов субъектов персональных данных или их представителей

30. При поступлении обращения субъекта финансовое управление должно зарегистрировать его в Журнале учета обращений субъектов персональных данных по форме согласно Приложению 17 к настоящему Положению.

31. Финансовое управление обязано сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя, либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его законного представителя.

32. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а - также таких персональных данных финансовое управление обязано дать в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его законного представителя, либо с даты получения запроса субъекта персональных данных или его законного представителя.

33. Финансовое управление обязано безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них

необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет финансовое управление, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах финансовое управление обязано уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

34. Финансовое управление обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

VIII. Основные условия проведения обработки персональных данных

35. Обработка персональных данных осуществляется после получения согласия субъекта персональных данных, составленного по форме согласно Приложению 1 к настоящему Положению, за исключением случаев, предусмотренных федеральным законом.

Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2, 3, 3.1, 4, 5, 6, 7, 8, 9, 9.1, 10, 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона.

36. Оператором ИСПДн финансовое управление, организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных является финансовое управление.

37. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

38. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн оператором назначается должностное лицо, ответственное за организацию обработки персональных данных в финансовом управлении.

Должностное лицо, ответственное за обеспечение безопасности персональных данных взаимодействует по вопросам организации защиты персональных данных в ИСПДн с отделом информационной безопасности администрации Уссурийского городского округа.

39. Руководитель финансового управления определяет должностных лиц, допущенных к обработке персональных данных.

40. Должностные лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно приложению 2 к Положению.

41. Оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Оператор или иное получившее доступ к персональным данным лицо обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

42. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности

персональных данных и безопасности персональных данных при их обработке.

IX. Способы обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации

43. Способы обработки персональных данных в ИСПДн финансового управления:

а) обработка персональных данных с использованием средств автоматизации;

б) обработка персональных данных без использования средств автоматизации;

в) исключительно автоматизированная обработка персональных данных;

г) смешанная обработка персональных данных.

X. Правила обработки и защиты персональных данных в информационных системах с использованием средств автоматизации

44. Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями, утвержденными Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

45. Оператор ИСПДн определяет тип угроз безопасности персональных данных, актуальных для ИСПДн, с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона, и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона.

46. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную

опасность несанкционированного, в том числе случайного доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

47. Угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

48. Угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

49. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

50. Оператор ИСПДн на основании типа угроз определяет уровень защищенности персональных данных в зависимости от категории обрабатываемых данных и их количества.

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

51. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа

и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

52. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора,

53. Необходимость обеспечения 3-го уровня защищенности

персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

54. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

55. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

56. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

а) утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем, и других нормативных и методических документов;

б) настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации

и других программных и технических средств в соответствии с требованиями безопасности информации;

в) охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

XI. Правила обработки и защиты персональных данных в информационных системах без использования средств автоматизации

57. Обработка персональных данных без использования средств автоматизации (в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации) осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

58. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

а) определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

б) обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

в) соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

59. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция

по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

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

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

60. При использовании внешних электронных носителей информации с персональными данными данные электронные носители информации, учитываются в журнале учета, выдачи и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, персональных данных в финансовом управлении.

61. Все документы, содержащие персональные данные, должны храниться в служебных помещениях в недоступных для посторонних лиц местах, надежно запираемых и опечатываемых шкафах (сейфах). При этом

должны быть созданы условия, обеспечивающие их сохранность.

ХII. Правила исключительно автоматизированной обработки персональных данных

62. При исключительно автоматизированной обработке персональных данных должны выполняться правила обработки персональных данных средствами автоматизации, указанные в разделе 10 настоящего Положения.

63. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

64. В остальных случаях принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, запрещается.

65. При исключительно автоматизированной обработке персональных данных необходимо:

а) разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных;

б) разъяснить возможные юридические последствия такого решения;

в) предоставить возможность заявить возражение против такого решения;

г) рассмотреть возражение;

д) уведомить субъекта персональных данных о результатах рассмотрения такого возражения в течение тридцати дней со дня получения

возражения.

ХIII. Правила смешанной обработки персональных данных

66. При смешанной обработке персональных данных необходимо выполнять правила объединяющие правила обработки персональных данных с использованием средств автоматизации, указанные в разделе 10 настоящего Положения, и правила обработки персональных данных без использования средств автоматизации, указанные в разделе 11 настоящего Положения.

ХIV. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных третьему лицу

67. Финансовое управление вправе поручить обработку персональных данных третьему лицу (поручение оператора):

а) с согласия субъекта персональных данных и если иное не предусмотрено федеральным законом;

б) на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Положением.

68. В поручении оператора:

а) должен быть определен перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;

б) должны быть определены цели обработки персональных данных;

в) должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных;

г) должна быть установлена обязанность такого лица обеспечивать безопасность персональных данных при их обработке;

д) должны быть указаны требования к защите обрабатываемых

персональных данных в соответствии с настоящим Положением и техническим заданием на создание системы защиты персональных данных;

е) должна быть установлена ответственность такого лица перед финансовым управлением, в случаях нарушений установленных требований и законодательства Российской Федерации в области персональных данных;

ж) при необходимости получения согласий на обработку персональных данных от субъектов персональных данных должен быть предусмотрен порядок сбора и передачи в финансовое управление таких согласий субъектов персональных данных.

69. В случае если финансовое управление поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет финансовое управление.

70. В случае необходимости получения согласия на обработку персональных данных от субъекта персональных данных, обязанность получения таких согласий возлагается на финансовое управление.

XV. Правила обработки обезличенных персональных данных

71. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

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

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

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

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

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

XVI. Правила обработки специальных категорий персональных данных

75. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частями 2 и 2.1 статьи 10 Федерального закона.

76. Обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления, в порядке и на условиях, которые предусмотрены Федеральным законом.

77. Обработка персональных данных о судимости может осуществляться финансовым управлением в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации.

78. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных пунктами 76 и 77, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

XVII. Правила обработки биометрических категорий персональных данных

79. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые

используются для установления личности субъекта персональных данных, могут обрабатываться в финансовом управлении только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных пунктом 80.

80. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

XVIII. Правила обработки персональных данных, разрешенных субъектом персональных данных для распространения, правила создания общедоступных источников персональных данных

81. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется только на основании согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения и с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных и может быть предоставлено:

а) непосредственно субъектом персональных данных по форме

согласно Приложению 19 к Положению;

б) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных, в соответствии с правилами, утвержденными Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 июня 2021 года № 106 «Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором.

Требования статьи 10.1 Федерального закона не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на финансовое управление функций, полномочий и обязанностей.

82. В целях информационного обеспечения в финансовом управлении могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных, по форме согласно приложению 18 к Положению, могут включаться его фамилия, имя, отчество, дата рождения, служебный номер телефона, занимаемая должность, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

83. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

XIX. Обеспечение безопасности персональных данных в финансовом управлении

84. С целью защиты субъектов персональных данных финансового управления от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или

преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи в финансовом управлении создается система безопасности персональных данных, включающая в себя организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

85. Система безопасности персональных данных финансового управления обеспечивает решение следующих задач:

а) своевременное выявление, оценка и прогнозирование источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба заинтересованным субъектам персональных данных, нарушению нормального функционирования ИСПДн финансового управления;

б) создание механизма оперативного реагирования на угрозы безопасности персональных данных;

в) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных;

г) защиту от вмешательства в процесс функционирования ИСПДн финансового управления посторонних лиц;

д) разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам финансового управления, то есть защиту от несанкционированного доступа;

е) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

ж) защиту от несанкционированной модификации используемых в ИСПДн финансового управления программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

з) защиту персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

и) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по обеспечению безопасности персональных данных при их обработке, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них.

86. В рамках реализации системы безопасности персональных данных в финансовом управлении проводятся следующие мероприятия:

а) строгий учет всех подлежащих защите ресурсов ИСПДн финансового управления (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

б) регистрация действий персонала, осуществляющего обслуживание и модификацию программных и технических средств ИСПДн;

в) разработка организационно-распорядительных документов по вопросам обеспечения безопасности информации;

г) подготовка должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

д) наделение каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ИСПДн финансового управления;

е) соблюдение всеми пользователями ИСПДн финансового управления требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

ж) несение персональной ответственности за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к ИСПДн финансового управления;

з) поддержание необходимого уровня защищенности элементов ИСПДн финансового управления;

и) применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

к) контроль над соблюдением пользователями ИСПДн финансового управления требований по обеспечению безопасности информации;

л) защита интересов финансового управления при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

XX. Контроль и надзор за соблюдением правил по обработке и защите персональных данных

87. Контроль и надзор за соблюдением правил по обработке и защите персональных данных в финансовом управлении состоит из следующих направлений:

а) внешний контроль и надзор за соблюдением правил по обработке и защите персональных данных;

б) внутренний контроль и надзор за соблюдением правил по обработке и защите персональных данных.

88. Внутренний контроль и надзор за соблюдением правил по обработке и защите персональных данных в администрации состоит из:

а) контроля и надзора за исполнением правил по обработке и защите персональных данных;

б) оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

89. Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется федеральным органом исполнительной власти, осуществляющим функции

по контролю и надзору в сфере информационных технологий и связи, федеральным органом исполнительной власти; уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

90. Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации в области защиты прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, подзаконных нормативных актов Правительства Российской Федерации, ведомственных нормативных актов и административных регламентов.

91. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

92. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

а) запрашивать у финансового управления информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

б) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных администрации, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

в) требовать от финансового управления уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем

персональных данных;

г) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства в области персональных данных;

д) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

е) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, необходимые сведения;

ж) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

з) привлекать к административной ответственности лиц, виновных в нарушении Федерального закона.

93. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

94. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

95. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области

противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

XXI. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в финансовом управлении

96. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в финансовом управлении организуется проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в финансовом управлении, на основании утвержденного Плана внутренних проверок условий обработки персональных данных в финансовом управлении.

97. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в финансовом управлении производится проверка:

- а) соблюдения принципов обработки персональных данных;
- б) соответствия нормативных правовых актов финансового управления в области персональных данных действующему законодательству Российской Федерации;
- в) выполнения сотрудниками финансового управления требований и правил обработки персональных данных в ИСПДн финансового управления;
- г) перечней персональных данных, используемых для решения задач и функций финансовым управлением, и необходимости обработки персональных данных в ИСПДн финансовом управлении;
- д) актуальности информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен

субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;

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

ж) актуальности перечня должностей сотрудников финансового управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

з) соблюдения прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных финансового управления;

и) соблюдения обязанностей финансового управления, предусмотренных действующим законодательством в области персональных данных;

к) порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных финансового управления, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

л) наличия необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных финансового управления;

м) актуальности сведений, содержащихся в уведомлении финансового управления об обработке персональных данных;

н) актуальности перечня информационных систем персональных данных в финансовом управлении;

о) знаний и соблюдения сотрудниками финансового управления положений действующего законодательства Российской Федерации, нормативных правовых актов администрации в области обработки и обеспечения безопасности персональных данных;

п) знаний и соблюдения сотрудниками финансового управления инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

р) соблюдения сотрудниками финансового управления конфиденциальности персональных данных;

с) актуальности нормативных актов финансового управления в области обеспечения безопасности персональных данных;

т) соблюдения сотрудниками финансового управления требований по обеспечению безопасности персональных данных;

у) наличия нормативных актов финансового управления, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных финансового управления;

ф) иных вопросов.

98. По результатам проведенной проверки оформляется Акт внутренней проверки состояния защиты персональных данных в финансовом управлении.

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

99. Во время осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в финансовом управлении производится оценка соотношения вреда, который может быть

причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в финансовом управлении.

100. При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, для каждой ИСПДн финансового управления производится экспертное сравнение заявленной финансовым управлением оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных и применяемых финансовым управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и изложенных в настоящем Положении.

101. По итогам сравнений принимается решение о достаточности применяемых финансовым управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных, и возможности или необходимости принятия дополнительных мер или изменения установленного в финансовом управлении порядка обработки и обеспечения безопасности персональных данных.

102. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в финансовом управлении оформляется в виде отдельного документа.

103. По результатам принятых решений лицом, ответственным за организацию обработки персональных данных в финансовом управлении организуется работа по их реализации.

XXIII. Ответственность должностных лиц

104. Сотрудники финансового управления, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

105. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение 1
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(Ф.И.О.)

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

выдан _____
(когда и кем)

проживающий(ая) по адресу: _____

в целях _____

_____ (цель обработки персональных данных)
даю согласие _____

_____ (наименование и адрес оператора)

на обработку моих персональных данных, а именно: _____

_____ (перечень персональных данных)

то есть на осуществление любых действий (операций) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных, в том числе на передачу, доступ, распространение, предоставление персональных данных определенному кругу лиц (в том числе, на обработку персональных данных по поручению оператора другому лицу):

_____ (наименование и адрес лица, осуществляющего обработку персональных данных по поручению оператора)

_____ (если обработка будет поручена такому лицу))

Настоящее согласие действует со дня его подписания и дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации. Настоящее согласие может быть отозвано в соответствии с законодательством Российской Федерации.

_____ (фамилия, инициалы лица, давшего согласие) _____ (подпись)

" ____ " _____ Г.

ОБЯЗАТЕЛЬСТВО
О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я, _____,
(Ф.И.О)

исполняющий(ая) должностные обязанности по замещаемой должности

(должность, наименование структурного подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

(фамилия, инициалы)

(подпись)

" " _____ г.

Разъяснение
субъекту персональных данных юридических последствий
отказа предоставить свои персональные данные

Уважаемый(ая) _____!

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

(реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям _____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия 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.

(должность)

(подпись)

(Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 4
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

(указать уполномоченный орган)

УВЕДОМЛЕНИЕ ОБ УНИЧТОЖЕНИИ

Настоящим уведомлением сообщаем Вам, что в связи с _____
_____ персональные данные _____
_____ (указать персональные данные)
уничтожены.

(должность) (подпись) (Ф.И.О.)

" " _____ 20__ г.

Приложение 5
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

(указать уполномоченный орган)

УВЕДОМЛЕНИЕ
ОБ УСТРАНЕНИИ ДОПУЩЕННЫХ НАРУШЕНИЙ

Настоящим уведомлением сообщаем Вам, что допущенные нарушения при
обработке персональных данных, а именно _____

(указать допущенные нарушения)
устранены.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 6
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

ЗАПРОС

Уважаемый(ая): _____ (Ф.И.О.), в связи с
_____ у финансового управления администрации Уссурийского
городского округа возникла необходимость получения следующей информации,
составляющей Ваши персональные данные _____

(перечислить информацию)

Просим Вас предоставить указанные сведения в течение _____ рабочих дней с
момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим в
указанный срок дать письменное согласие на получение нами необходимой
информации из следующих источников _____,
следующими способами _____.

По результатам обработки указанной информации нами планируется принятие
следующих решений, которые будут доведены до Вашего сведения.

Против принятого решения Вы имеете право заявить свои письменные
возражения в _____ срок.

_____ (должность)

_____ (подпись)

_____ (Ф.И.О.)

"__" _____ 20__ г.

УВЕДОМЛЕНИЕ О БЛОКИРОВАНИИ

Уважаемый(ая) _____ (Ф.И.О.),
в связи с _____ сообщаем Вам, что Ваши
персональные данные _____
(указать персональные данные)
заблокированы на срок _____.

(должность) (подпись) (Ф.И.О.)

" " _____ 20__ г.

Приложение 8
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

УВЕДОМЛЕНИЕ ОБ УТОЧНЕНИИ

Уважаемый(ая) _____ (Ф.И.О.), в связи с
_____ сообщаем Вам, что Ваши персональные данные
уточнены в соответствии со сведениями: _____.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 9
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

УВЕДОМЛЕНИЕ

Уважаемый(ая) _____ (Ф.И.О.),
финансовым управлением администрации Уссурийского городского округа
производится обработка сведений, составляющих Ваши персональные данные:

_____ (указать сведения)

Цели обработки: _____.

Способы обработки: _____.

Перечень лиц, которые имеют доступ к информации, содержащей Ваши
персональные данные или могут получить такой доступ:

№	Должность	Ф.И.О.	Вид доступа	Примечания

По результатам обработки указанной информации нами планируется принятие
следующих решений, которые будут доведены до Вашего сведения.

Против принятого решения Вы имеете право заявить свои письменные
возражения в _____ срок.

_____ (должность)

_____ (подпись)

_____ (Ф.И.О.)

" ____ " _____ 20__ г.

УВЕДОМЛЕНИЕ ОБ УНИЧТОЖЕНИИ

Уважаемый(ая) _____ (Ф.И.О.),
в связи с _____ сообщаем
Вам, что Ваши персональные данные _____

_____ (указать персональные данные)
уничтожены.

_____ (должность) _____ (подпись) _____ (Ф.И.О.)

"__" _____ 20__ г.

УВЕДОМЛЕНИЕ
ОБ УСТРАНЕНИИ ДОПУЩЕННЫХ НАРУШЕНИЙ

Уважаемый(ая) _____ (Ф.И.О.), в
связи с _____ сообщаем
Вам, что все допущенные нарушения при обработке Ваших персональных данных
устранены.

(должность)

(подпись)

(Ф.И.О.)

" " _____ 20__ г.

Приложение 12
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу заблокировать обрабатываемые Вами мои персональные данные:

_____ (указать блокируемые персональные данные)
на срок: _____ ;
_____ (указать срок блокирования)
в связи с тем _____
_____ (указать причину блокирования персональных данных)

(должность)

(подпись)

(Ф.И.О.)

" " _____ 20__ г.

Приложение 14
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты документа,
удостоверяющего личность заявителя)

ЗАЯВЛЕНИЕ

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки; предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ); сведения о том, какие юридические последствия для меня может повлечь ее обработка. В случае отсутствия такой информации, прошу Вас уведомить меня об этом.

(должность)

(подпись)

(Ф.И.О.)

"__" _____ 20__ г.

Приложение 15
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями: _____;

_____;
(указать уточненные персональные данные заявителя)

в связи с тем, что _____.
(указать причину уточнения персональных данных)

(должность)

(подпись)

(Ф.И.О.)

" ____ " _____ 20__ г.

Приложение 16
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

В _____
от _____
(Ф.И.О. заявителя)

(наименование и реквизиты
документа, удостоверяющего
личность заявителя)

ЗАЯВЛЕНИЕ

Прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями: _____;

_____;
(указать уточненные персональные данные заявителя)

в связи с тем, что _____.
(указать причину уточнения персональных данных)

(должность)

(подпись)

(Ф.И.О.)

" " _____ 20__ г.

Приложение 17
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

ЖУРНАЛ
УЧЕТА ОБРАЩЕНИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Журнал начат "___" _____ 20__ г. Журнал завершён "___" _____ 20__ г.
_____/Должность/ _____/Должность/
_____/Ф.И.О., подпись/ _____/Ф.И.О., подпись/

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи/отказа в предоставлении информации	Подпись ответственного лица	Примечание
1							
2							
3							
4							
5...							

Приложение 18
к Положению
по обеспечению безопасности
персональных данных в
финансовом управлении
администрации Уссурийского
городского округа

Согласие

на включение персональных данных в общедоступные источники персональных данных финансового управления администрации Уссурийского городского округа

Я, _____,
(Ф.И.О.)

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

выдан _____,
(когда и кем)

проживающий(ая) по адресу: _____

в целях _____,
(цель обработки персональных данных)

даю согласие _____,
(наименование и адрес оператора)

считать следующие персональные данные общедоступными:

(перечислить персональные данные)

Согласен на осуществление любых действий (операций) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с моими общедоступными персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных, в том числе на передачу, доступ, распространение, предоставление персональных данных определенному кругу лиц.

Настоящее согласие действует со дня его подписания и дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

Настоящее согласие может быть отозвано в соответствии с законодательством Российской Федерации.

(фамилия, инициалы лица, давшего согласие)

(подпись)

" " _____ г.

Приложение 19
к Положению
по обеспечению безопасности
персональных данных в
администрации Уссурийского
городского округа

СОГЛАСИЕ
на обработку персональных данных,
разрешенных субъектом персональных данных для распространения

Я, _____,

(Ф.И.О)

серия _____ № _____

(вид документа, удостоверяющего личность)

выдан _____,

(когда и кем)

проживающий (ая) по адресу: _____

в целях _____

(цель распространения персональных данных)

даю согласие

(наименование и адрес оператора)

на распространение моих персональных данных неограниченному кругу лиц:

(категории и перечень персональных данных)

общие персональные данные: _____

_____;

специальные категории персональных данных: _____

_____;

биометрические персональные данные: _____

_____.

Категории и перечень персональных данных, для обработки которых устанавливаются условия и запреты, а также перечень устанавливаемых условий и запретов (за исключением предоставления и получения доступа), в том числе условия, при которых персональные данные могут передаваться только по внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников оператора:

_____.

Сведения об информационных ресурсах, посредством которых будет осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

(адрес информационного ресурса (сайта, страницы сайта))

Настоящее согласие дано мной добровольно и действует со дня его подписания и дается на период до _____
(дата окончания или период действия)

Настоящее согласие может быть отозвано мною в соответствии с законодательством Российской Федерации. В случае получения требования оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

(фамилия, инициалы лица, давшего согласие)

(подпись)

« _____ » _____ Г.