



**ДЕПАРТАМЕНТ ФИНАНСОВО-БЮДЖЕТНОГО НАДЗОРА
КРАСНОДАРСКОГО КРАЯ**

П Р И К А З

от 24.11.2020

№ 145

г. Краснодар

**Об организационных мероприятиях по обработке
и обеспечению безопасности персональных данных,
обрабатываемых в департаменте финансово-бюджетного надзора
Краснодарского края**

Во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с постановлениями Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. № 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», п р и к а з ы в а ю :

1. Утвердить руководящие документы департамента финансово-бюджетного надзора Краснодарского края (далее – департамент) по защите персональных данных:

1) Правила обработки персональных данных в департаменте (приложение 1).

2) Правила рассмотрения запросов субъектов персональных данных или их представителей в департаменте (приложение 2).

3) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в департаменте (приложение 3).

4) Правила доступа в помещения департамента, в которых ведётся обработка защищаемой информации, в том числе персональных данных (приложение 4).

5) Перечень персональных данных, обрабатываемых в департаменте (приложение 5).

6) Перечень должностей департамента, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 6).

7) Перечень информационных ресурсов и систем департамента, а также сведений, обрабатываемых в них (приложение 7).

8) Оценку вреда, который может быть причинён субъектам персональных данных департамента (приложение 8).

2. Утвердить типовые формы документов по защите персональных данных, обрабатываемых в департаменте:

1) Типовая форма согласия на обработку персональных данных (приложение 9).

2) Типовая форма разъяснения субъекту персональных данных (замещающего должности гражданского государственного служащего) юридических последствий отказа предоставить свои персональные данные (приложение 10).

3) Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение 11).

4) Типовое обязательство сотрудника департамента, непосредственно осуществляющего обработку персональных данных (приложение 12).

3. Главному консультанту отдела кадровой работы, противодействия коррупции, учета и материально-технического обеспечения Голикову Леониду Вадимовичу ознакомить под роспись сотрудников департамента, осуществляющих обработку персональных данных с Правилами обработки персональных данных в департаменте.

4. Отделу кадровой работы, противодействия коррупции, учета и материально-технического обеспечения (Голиков Л.В.) обеспечить размещение (опубликование) на официальном сайте администрации Краснодарского края в информационно-телекоммуникационной сети «Интернет», на официальном сайте департамента и направление на «Официальный интернет-портал правовой информации» (www.pravo.gov.ru) следующие документы, определяющие политику департамента, в отношении обработки персональных данных:

1) Приказ «Об организационных мероприятиях по обработке и обеспечению безопасности персональных данных, обрабатываемых в департаменте финансово-бюджетного надзора Краснодарского края»

2) Правила обработки персональных данных в департаменте, в отношении обработки персональных данных (приложение 1).

3) Правила рассмотрения запросов субъектов персональных данных или их представителей в департаменте, в отношении обработки персональных данных (приложение 2).

5. Назначить ответственным за организацию обработки персональных данных в департаменте, главного консультанта отдела кадровой работы, противодействия коррупции, учета и материально-технического обеспечения Голикова Л. В.

6. Признать утратившими силу:

1) приказ департамента финансово-бюджетного надзора Краснодарского края от 2 июня 2014 г. № 31 «Об утверждении правил обработки персональных

данных в департаменте финансово-бюджетного надзора Краснодарского края»;

2) приказ департамента финансово-бюджетного надзора Краснодарского края от 2 марта 2015 г. №11 «Об утверждении порядка обеспечения основных мер безопасности в информационной системе персональных данных в департаменте финансово-бюджетного надзора Краснодарского края».

7. Контроль за выполнением настоящего приказа оставляю за собой.

8. Приказ вступает в силу на следующий день после его официального опубликования.

Руководитель департамента



В.В. Косенков

Приложение 1
к приказу департамента
финансово-бюджетного надзора
Краснодарского края
от 24.11.2020 № 145

ПРАВИЛА
обработки персональных данных в
департаменте финансово-бюджетного надзора
Краснодарского края

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в департаменте финансово-бюджетного надзора Краснодарского края (далее – Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Настоящие Правила разработаны в соответствии с:

Конституцией Российской Федерации;

Трудовым кодексом Российской Федерации;

Федеральным законом Российской Федерации от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее – Федеральный закон «О государственной гражданской службе Российской Федерации»);

Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»);

Федеральным законом Российской Федерации от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее - Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»);

Федеральным законом Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» (далее - Федеральный закон «О противодействии коррупции»);

Указом Президента Российской Федерации от 30 мая 2005 г. № 609

«Об утверждении Положения о персональных данных гражданского государственного служащего Российской Федерации и ведении его личного дела» (далее - Указ № 609);

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее - Постановление Правительства Российской Федерации № 687);

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» (далее - Постановление Правительства Российской Федерации № 211);

постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - Постановление Правительства Российской Федерации № 1119);

законом Краснодарского края от 31 мая 2005 г. № 870-КЗ «О государственной гражданской службе Краснодарского края».

2. Термины и определения

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

2.2. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

2.3. Биометрические персональные данные – персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (за исключением сведений, относящихся к специальным категориям персональных данных).

2.4. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.5. Иные персональные данные – любая информация, относящаяся к прямо или косвенно определённом, или определяемому физическому лицу

(субъекту персональных данных), за исключением персональных данных, относящихся к специальным, биометрическим или общедоступным персональным данным.

2.6. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.7. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

2.9. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

2.10. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

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

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

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

3. Принципы обработки персональных данных

3.1. Обработка персональных данных в департаменте финансово-бюджетного надзора Краснодарского края (далее – департамент) осуществляется в соответствии с настоящими Правилами, а также требованиями, установленными законодательством Российской Федерации с учётом необходимости обеспечения защиты прав и свобод субъектов

персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

обработка персональных данных осуществляется департаментом в связи с осуществлением функций, возложенных на него, а также реализацией служебных или трудовых отношений;

обработка персональных данных в департаменте осуществляется лицом (лицами), уполномоченным (и) приказом департамента на обработку персональных данных и несущим(и) ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных (далее - лицо, уполномоченное на обработку персональных данных);

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

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

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

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

содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки;

не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

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

принимаются необходимые меры, либо обеспечивается их принятие по удалению или уточнению неполных, или неточных персональных данных;

хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того 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 уничтожаются, либо обезличиваются по достижении целей обработки или, в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Лицо, уполномоченное на обработку персональных данных, обязано:

знать и выполнять требования законодательства в области персональных данных;

хранить в тайне известные ему персональные данные, информировать лицо, ответственное за организацию обработки персональных данных в Департаменте, о фактах нарушения порядка обращения с персональными

данными, о попытках несанкционированного доступа к ним;

соблюдать требования настоящих Правил, порядок учета и хранения персональных данных, исключать доступ к ним посторонних лиц;

обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей;

прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей в случае расторжения с ним служебного контракта.

3.3. Лицу, уполномоченному на обработку персональных данных, запрещается:

использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях - при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;

передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных ФСБ России средств криптографической защиты информации;

выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, за пределы места (помещения) их хранения;

нарушать режим защиты персональных данных.

3.4. Обработка персональных данных в департаменте осуществляется как с использованием средств автоматизации (в информационных системах), так и без использования таких средств и включает: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление и изменение, связанные с необходимостью их актуализации), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется лицом, уполномоченным на обработку персональных данных, путем:

получения оригиналов необходимых документов;

копирования оригиналов документов;

внесения сведений в учетные формы (на материальных и электронных носителях);

внесения персональных данных в установленном порядке в информационные системы, используемые в департаменте.

3.6. Трансграничная передача персональных данных в департаменте не осуществляется.

3.7. Принятие решений, порождающих юридические последствия в отношении субъектов персональных данных или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных, не осуществляется.

3.8. Перечень информационных систем, в которых осуществляется обработка персональных данных, представлен в приложении 1.

3.9. Субъектами персональных данных, чьи персональные данные обрабатываются в департаменте являются:

государственные гражданские служащие департамента;

граждане, претендующие на замещение вакантных должностей государственной гражданской службы;

граждане, обратившиеся в департамент в порядке, предусмотренном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»:

граждане, заключающие государственные контракты.

4. Условия и порядок обработки персональных данных государственных гражданских служащих и граждан, претендующих на замещение вакантных должностей государственной гражданской службы в департаменте

4.1. Персональные данные: лиц, замещающих в департаменте должности государственной гражданской службы Краснодарского края (далее - гражданские служащие); лиц, претендующих на замещение в департаменте должностей государственной гражданской службы Краснодарского края; лиц, состоящих в кадровом резерве департамента, обрабатываются в соответствии с Указом Президента РФ от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»

5. Условия и порядок обработки персональных данных граждан, обратившихся в Департамент в порядке, предусмотренном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»

5.1. Обработка персональных данных граждан, обратившихся в департамент в порядке, предусмотренном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», осуществляется в целях рассмотрения устных и письменных обращений граждан по вопросам, относящимся к компетенции департамента, с последующим уведомлением граждан о результатах рассмотрения, и в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

5.2. В соответствии с законодательством Российской Федерации в департаменте подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан, лиц без гражданства, а также обращения организаций.

5.3. В соответствии со статьями 7 и 13 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» при рассмотрении

обращений граждан Российской Федерации, иностранных граждан, лиц без гражданства подлежат обработке их следующие персональные данные:

фамилия, имя, отчество (последнее при наличии);

почтовый адрес;

адрес электронной почты;

указанный в обращении контактный телефон;

иные персональные данные, указанные в обращении, а также ставшие известными в ходе личного приема граждан или в процессе рассмотрения обращения.

5.4. Обработка персональных данных, необходимых в связи с рассмотрением обращений граждан, в соответствии с пунктом 2 части 1 статьи 6 Федерального закона «О персональных данных» и Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», осуществляется без согласия субъектов персональных данных.

5.5. Обработка вышеуказанных персональных данных граждан, осуществляется должностными лицами департамента путём:

получения обращения в электронном и письменном виде;

получения оригиналов необходимых документов;

предоставления заверенных в установленном порядке копий документов;

получения необходимых для рассмотрения обращения документов и материалов в органах государственной власти, органах местного самоуправления, у иных должностных лиц, за исключением судов, органов дознания и органов предварительного следствия;

внесения сведений в учётные формы (на бумажных и электронных носителях);

внесения персональных данных в информационные системы Департамента.

5.6. Использование персональных данных заявителей осуществляется Департаментом в случаях и в порядке, предусмотренных Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

5.7. Передача (предоставление) персональных данных заявителей осуществляется департаменте в случаях и в порядке, предусмотренных частью 3 статьи 8 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации».

6. Процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в сфере защиты персональных данных

6.1. Процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в сфере защиты персональных данных, включают в себя выполнение обязанностей и реализацию комплекса мер по обеспечению безопасности персональных данных департамента, предусмотренных Федеральным законом «О

персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и включают в себя:

назначение лица, ответственного за обработку персональных данных в Департаменте;

сбор согласий (в соответствии с установленной типовой формой) на обработку персональных данных, в случаях, установленных действующим законодательством Российской Федерации и настоящими Правилами;

оценку вреда, который может быть причинён субъектам персональных данных департамента;

обезличивание, уточнение и уничтожение персональных данных, в случаях, когда это необходимо;

определение правил рассмотрения запросов субъектов персональных данных или их представителей;

определение правил работы с обезличенными данными в случае обезличивания персональных данных;

определение порядка доступа в помещения, департамента, в которых ведётся обработка персональных данных;

осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами департамента;

определение угроз безопасности персональных данных, при их обработке в информационных системах департамента;

определение уровня защищённости персональных данных, обрабатываемых в информационных системах департамента;

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

исключение несанкционированного, в том числе случайного, доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных;

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

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

учёт машинных носителей персональных данных;

обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

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

установление правил доступа к персональным данным, а также обеспечением регистрации и учёта всех действий, совершаемых с

персональными данными в информационных системах Департамента;
контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

7. Полномочия лица, ответственного за организацию обработки персональных данных в департаменте

7.1. Ответственный за организацию обработки персональных данных в департаменте, назначается приказом руководителя департамента.

7.2. Ответственный за организацию обработки персональных данных в департаменте, обязан:

организовывать принятие мер, необходимых для обеспечения защиты в департаменте обрабатываемых персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;

осуществлять внутренний контроль, за соблюдением в департаменте требований законодательства в области персональных данных, в том числе требований к защите персональных данных;

обеспечить доведение до сведения лиц, непосредственно связанных с реализацией настоящих Правил, положений законодательства в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

организовать прием и обработку обращений (запросов) субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений (запросов);

в случае нарушения в департаменте требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

7.3. Лицо, ответственное за организацию обработки персональных данных в департаменте, вправе:

В установленном порядке привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в департаменте, в том числе для проведения внутренних проверок, государственных гражданских служащих с возложением на них соответствующих обязанностей и закреплением ответственности;

Иметь доступ к информации, касающейся обработки персональных данных в Департаменте и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых в департаменте способов обработки персональных данных;

описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
дату начала обработки персональных данных;
срок или условия прекращения обработки персональных данных;
сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении положений законодательства в области персональных данных, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и (или) уголовной ответственности в порядке, установленном федеральными законами.

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

Приложение 1
к правилам обработки
персональных данных в
департаменте финансово-
бюджетного надзора
Краснодарского края

ПЕРЕЧЕНЬ
информационных систем, в которых осуществляется
обработка персональных данных в департаменте финансово-
бюджетного надзора Краснодарского края

В департаменте функционируют (эксплуатируются) следующие информационные системы:

1. Информационная система «1С: Бухгалтерия»;
2. Информационная система «1С: Зарплата и кадры»;
3. Федеральная государственная информационная система «Госслужба»;
4. Государственная информационная система «Электронный бюджет»;
5. Единая межведомственная система электронного документооборота Краснодарского края;
6. Автоматизированная система «Удаленное Рабочее Место»;
7. Система удаленного финансового документооборота;
8. Автоматизированная система «Web-Консолидация»;
9. Государственная информационная система о государственных и муниципальных платежах;
10. Региональная информационная система в сфере закупок Краснодарского края;
11. Информационная система «Сетевой Справочный Телефонный Узел»;
12. Система электронного документооборота «Обращения граждан»;
13. Программный комплекс «Web-планирование»;
14. Единая информационная система «Закупки»;
15. Информационная система «Сбербанк Бизнес Онлайн»;
16. Информационная система «Контур - экстерн»;
17. Государственная информационная система «Мой Арбитр»;
18. ГИС в области гражданской службы Краснодарского края

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

ПРАВИЛА
рассмотрения запросов субъектов персональных данных
или их представителей в департаменте финансово-бюджетного надзора
Краснодарского края

1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в департаменте финансово-бюджетного надзора Краснодарского края (далее – Правила) определяют порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы) в департаменте финансово-бюджетного надзора Краснодарского края (далее – департамент).

1.2. Настоящие Правила разработаны в соответствии с:
трудовым кодексом Российской Федерации;
Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»);

Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее – Федеральный закон «О государственной гражданской службе Российской Федерации»);

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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.

1.3. Настоящие Правила распространяются на сотрудников Департамента, осуществляющих работу с гражданами, претендующих на замещение вакантных должностей, обратившихся в департамент в порядке,

предусмотренном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», заключающих государственные контракты.

2. Права субъектов персональных данных

2.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных», в том числе содержащей:

подтверждение факта обработки персональных данных в департаменте;

правовые основания и цели обработки персональных данных;

цели и применяемые в департаменте способы обработки персональных данных;

наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора, то есть помимо работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с департаментом или на основании Федерального закона, в соответствии с которым осуществляется предоставление персональных данных;

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

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

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

информацию об осуществлённой или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом «О государственной гражданской службе Российской Федерации».

2.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных».

2.3. Субъект персональных данных вправе требовать от департамента уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные Федеральным законом «О персональных данных» меры по защите своих прав.

2.4. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», должны быть предоставлены субъекту персональных

данных в доступной форме и в них не должно содержаться персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

2.5. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», предоставляются субъекту персональных данных или его представителю департаментом, при обращении субъекта персональных данных, либо при получении запроса субъекта персональных данных или его представителя.

3. Правила рассмотрения запросов субъектов

3.1. Запрос субъекта персональных данных должен содержать:
номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

сведения о дате выдачи указанного документа и выдавшем его органе;

сведения, подтверждающие участие субъекта персональных данных в отношениях с департаментом, либо сведения, иным образом подтверждающие факт обработки персональных данных департаментом, подпись субъекта персональных данных или его представителя.

3.2. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации, согласно форме, приведённой в приложении 1.

3.3. Рассмотрение запросов является обязанностью уполномоченных сотрудников департамента.

3.4. Сотрудники департамента обеспечивают:

проверку достоверности сведений, указанных в запросе;

объективное, всестороннее и своевременное рассмотрение запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

3.5. Запрос прочитывается и проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в департамент или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», и ознакомления с такими персональными данными в соответствии с частью 4 статьи 14 Федерального закона «О персональных данных» не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен предусмотренным Федеральным законом «О порядке рассмотрения обращений

граждан Российской Федерации», Федеральным законом «О государственной гражданской службе Российской Федерации».

3.6. Срок предоставления ответов на поступившие запросы от субъектов персональных данных или их представителей в соответствии с частью 1 статьи 20 Федерального закона «О персональных данных» составляет тридцать дней.

3.7. Субъект персональных данных вправе обратиться повторно в департамент или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ «О персональных данных», а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объёме по результатам рассмотрения первоначального обращения. Повторный запрос, наряду с необходимыми сведениями, должен содержать обоснование направления повторного запроса.

3.8. Департамент вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным.

3.9. Департамент обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя, либо дать письменный ответ, согласно форме, приведённой в приложении № 2, в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

3.10. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя, уполномоченные должностные лица департамента обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного Федерального закона, являющегося основанием для такого отказа, согласно форм отказов, приведённых в приложении № 3, № 4.

3.11. Департамент обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

3.12. В соответствии с частью 3 статьи 20 Федерального закона «О персональных данных» департамент:

в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений,

подтверждающих, что персональные данные являются неполными, неточными или неактуальными, сотрудники департамента обязаны внести в них необходимые изменения;

в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, сотрудники департамента обязаны уничтожить такие персональные данные.

3.13. Департамент обязан уведомить субъекта персональных данных или его представителя о внесённых изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.14. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, сотрудники департамента обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

3.15. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, сотрудники департамента обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.16. В случае подтверждения факта неточности персональных данных сотрудники департамента на основании сведений, представленных субъектом персональных данных или его представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в соответствии с частью 2 статьи 20 Федерального закона «О персональных данных» в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

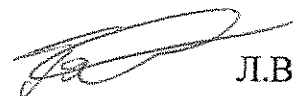
3.17. В случае выявления неправомерной обработки персональных данных сотрудники департамента в срок, в соответствии с частью 3 статьи 20 Федерального закона «О персональных данных», не превышающий трёх рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных, а в случае, если обеспечить правомерность обработки персональных данных невозможно, сотрудники Департамента в срок не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных обязаны уничтожить такие персональные

данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Департамент обязан уведомить субъекта персональных данных или его представителя. В случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган.

3.18. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

3.19. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками департамента действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация передается незамедлительно в правоохранительные органы. Служебная проверка проводится в соответствии с законодательством Российской Федерации.

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

Приложение 1
к правилам рассмотрения
запросов субъектов
персональных данных
или их представителей в
департаменте финансово-
бюджетного надзора
Краснодарского края

ФОРМА

Руководителю департамента финансово-
бюджетного надзора Краснодарского края

Ф.И.О. субъекта персональных данных

Номер основного документа, удостоверяющего личность

Наименование выдавшего органа

Дата выдачи

**Заявление (запрос) о доступе субъекта
персональных данных к своим персональным данным**

Прошу подтвердить факт обработки моих персональных данных и
предоставить мне для ознакомления информацию, составляющую мои
персональные данные, на основании:

(указать сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора,
дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом
подтверждающие факт обработки персональных данных оператором)

дата

подпись

расшифровка подписи

Приложение 2
к правилам рассмотрения
запросов субъектов
персональных данных или
их представителей в
департаменте финансово-
бюджетного надзора
Краснодарского края

ФОРМА

**Ответ на запрос о предоставлении субъекту
его персональных данных**

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

В ответ на Ваш запрос от _____
(дд.мм.гг.)

сообщаем, что в департаменте финансово-бюджетного надзора Краснодарского края (далее – Оператор), расположенный по адресу: г. Краснодар, ул. Короленко, дом 2\1, осуществляется обработка следующих Ваших персональных данных:

(перечислить персональные данные)

Указанные персональные данные получены

(непосредственно от Вас / указать источник получения персональных данных)

Персональные данные обрабатываются и используются Оператором в целях и на _____ основании

(перечислить цели и правовые основания обработки)

Ваши персональные данные обрабатываются (нужное подчеркнуть) автоматизированным / неавтоматизированным / смешанным способом.

Перечень лиц (за исключением работников Оператора), которые имеют доступ к Вашим персональным данным или которым могут быть раскрыты

Ваши персональные данные на основании договора с оператором или на основании федерального закона:

(перечислить юридические и физические лица)

Сроки обработки и хранения персональных данных определяются целями обработки (персональные данные обрабатываются до тех пор, пока соответствуют целям обработки).

дата	подпись	расшифровка подписи
------	---------	---------------------

Настоящее уведомление на руки получил(а):

дата	подпись	расшифровка подписи
------	---------	---------------------

Приложение 3
к правилам рассмотрения
запросов субъектов
персональных данных или
их представителей в
департаменте финансово-
бюджетного надзора
Краснодарского края

ФОРМА

**Отказ в выполнении повторного запроса
субъекта персональных данных**

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

На основании _____

(ссылка на положение части 4 или 5 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных"
или на иной федеральный закон, являющийся основанием для такого отказа)

департамент финансово-бюджетного надзора Краснодарского края вынужден
отказать Вам в выполнении повторного запроса на доступ к Вашим
персональным данным.

дата

подпись

расшифровка подписи

Настоящее уведомление на руки получил(а):

дата

подпись

расшифровка подписи

Приложение 4
к правилам рассмотрения
запросов субъектов
персональных данных или
их представителей в
департаменте финансово-
бюджетного надзора
Краснодарского края

ФОРМА

**Отказ в предоставлении доступа субъекта
персональных данных к его персональным данным**

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

На основании _____

(ссылка на положение части 8 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" или
на иной федеральный закон, являющийся основанием для такого отказа)

департамент финансово-бюджетного надзора Краснодарского края вынужден
отказать Вам в предоставлении доступа к Вашим персональным данным.

дата

подпись

расшифровка подписи

Настоящее уведомление на руки получил(а):

дата

подпись

расшифровка подписи

ПРАВИЛА
осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных в департаменте финансово-бюджетного
надзора Краснодарского края

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в департаменте финансово-бюджетного надзора Краснодарского края (далее - Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Настоящие Правила разработаны в соответствии с:

Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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;

постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящими Правилами в своей работе должны руководствоваться:

сотрудники департамента финансово-бюджетного надзора Краснодарского края (далее - департамент), осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

2. Структура процессов по внутреннему контролю

2.1. Контроль выполнения требований по защите персональных данных в структурных подразделениях департамента осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

2.2. Контроль выполнения требований по защите персональных данных в структурных подразделениях департамента осуществляет ответственный за организацию обработки персональных данных в департаменте и администратор информационной безопасности Департамента.

2.3. Общий контроль выполнения требований по обеспечению безопасности персональных данных осуществляет ответственный за выполнение мероприятий по контролю исполнения в структурных подразделениях департамента требований документов по обеспечению безопасности персональных данных.

2.4. Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

2.5. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

2.6. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных или нарушения требований по защите персональных данных.

2.7. Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений департамента не позднее, чем за 24 часа до начала проверки.

2.8. Проверки по частным вопросам могут проводиться без уведомления руководителей структурных подразделений департамента.

2.9. Периодичность и сроки проведения плановых проверок структурных подразделений департамента устанавливаются планом проверок на календарный год. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

3. Порядок подготовки к проверке

3.1. Общий контроль выполнения требований по обеспечению безопасности персональных данных в структурных подразделениях департамента осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных департамента (форма представлена в приложении 1), утвержденным руководителем департамента финансово-бюджетного надзора Краснодарского края.

3.2. Ответственный за выполнение мероприятий по контролю исполнения структурных подразделений департамента требований документов по обеспечению безопасности персональных данных подготавливает предложения по составу комиссии или группы проверяющих лиц.

3.3. Контроль в структурных подразделениях департамента, осуществляемый ответственными за обеспечение контроля процессов обеспечения безопасности персональных данных структурных подразделений департамента, осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений департамента (форма представлена в приложении 2). Данные Планы утверждаются руководителями структурных подразделений департамента и согласовываются с ответственным за выполнение мероприятий по контролю исполнения структурных подразделений департамента, требований документов по обеспечению безопасности персональных данных.

3.4. Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений департамента информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения департамента.

4. Порядок проведения проверки

4.1. Руководитель проверяемого структурного подразделения департамента обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

4.2. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

4.3. Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких сотрудников структурных подразделений департамента необходимо привлечь к проверке и какие помещения следует посетить.

4.4. Общий порядок проведения проверки включает:

выявление сотрудников, задействованных в обработке персональных данных;

проверка факта ознакомления сотрудников проверяемого структурного подразделения департамента с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных;

получение при содействии сотрудников проверяемого структурного подразделения департамента документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

анализ полученной документации;

непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

4.5. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении департамента рассматриваются следующие показатели работ по защите персональных данных:

наличие согласий на обработку персональных данных субъектов персональных данных, в случаях, предусмотренных законодательствам Российской Федерации;

соответствие состава и сроков обработки целям обработки ПДн;

соответствие Перечня должностей государственных гражданских служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным реальному составу сотрудников;

соответствие Перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных реальному составу сотрудников;

наличие нормативных документов по защите персональных данных;

знание нормативных документов и уровень подготовки сотрудников, имеющих доступ к персональным данным;

полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;

наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных;

4.6. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении департамента дополнительно рассматриваются следующие показатели работ по защите персональных данных:

соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

наличие и корректность перечня информационных систем;

наличие документа, подтверждающего:

правильность определения уровня защищенности персональных данных, обрабатываемых в информационных системах, а также классов защищенности информационных систем;

наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность (срок актуальности документа не может превышать 3 года);

соответствие состава средств вычислительной техники информационных систем указанному в документации на информационную систему;

соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);

порядок защиты персональных данных при передаче по сети;

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

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

4.7. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

4.8. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

5. Оформление результатов проверки

5.1. Результаты проверки оформляются актом.

5.2. Акт составляется в одном экземпляре и подписывается членами комиссии. Оригинал документа с результатами проверки хранится (передается) у ответственного за выполнение мероприятий по контролю исполнения структурными подразделениями департамента требований документов по обеспечению безопасности персональных данных. Копия документа о проверке передается в проверяемое структурное подразделение департамента.

5.3. Результаты проверок подразделений периодически обобщаются ответственным за выполнение мероприятий по контролю исполнения структурными подразделениями департамента и доводятся до сведения ответственного за организацию обработки и обеспечение безопасности персональных данных департамента.

5.4. При необходимости принятия решений по результатам проверки структурного подразделения департамента – ответственному за организацию обработки и обеспечение безопасности персональных данных департамента готовится соответствующая служебная записка.

6. Корректирующие мероприятия и контроль за их исполнением

6.1. Руководитель структурного подразделения департамента анализирует акт о результатах внутренней проверки и в пятидневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

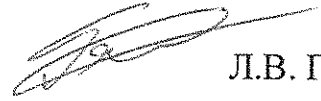
6.2. Перечень мероприятий согласуется с ответственным за организацию обработки и обеспечение безопасности персональных данных департамента.

6.3. Если корректирующие мероприятия касаются других структурных подразделений департамента, то к анализу привлекаются специалисты соответствующих структурных подразделений.

6.4. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки и обеспечение безопасности персональных данных департамента.

6.5. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Главный консультант отдела кадровой
работы, противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

Приложение 1

к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к защите
персональных данных
в департаменте финансово-бюджетного
надзора Краснодарского края

ПЛАН

**проведения внутренних проверок соответствия обработки
персональных данных требованиям к защите персональных
данных департамента финансово-бюджетного надзора
Краснодарского края**

№ п/п	Наименование структурного подразделения департамента финансово-бюджетного надзора Краснодарского края	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6	7

Заместитель руководителя департамента финансово-
бюджетного надзора Краснодарского края



Л.В. Крылова

Приложение 2
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к защите
персональных данных
в департаменте финансово-бюджетного
надзора Краснодарского края

ПЛАН
проведения внутренних проверок соответствия обработки
персональных данных требованиям к защите персональных
данных структурных подразделений департамента финансово-
бюджетного надзора Краснодарского края

№ п/п	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6

Заместитель руководителя департамента финансово-
бюджетного надзора Краснодарского края



Л.В. Крылова

ПРАВИЛА

доступа в помещения департамента финансово-бюджетного надзора Краснодарского края, в которых ведётся обработка защищаемой информации, в том числе персональных данных

1. Общие положения

1.1. Настоящие Правила устанавливают порядок доступа в помещения департамента финансово-бюджетного надзора Краснодарского края (далее – департамент), в которых ведётся обработка конфиденциальной и защищаемой информации, в том числе персональных данных (далее – Информация).

1.2. Правила разработаны в целях обеспечения безопасности информации, обрабатываемой в департаменте, на средствах вычислительной техники информационных систем, на материальных носителях информации, а также для обеспечения внутриобъектового режима.

1.3. Настоящий Порядок устанавливает правила доступа в следующие помещения департамента:

помещения, в которых происходит обработка Информации, как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

помещения, в которых хранятся материальные носители Информации и их резервные копии;

помещения, в которых установлены средства криптографической защиты информации (далее – СКЗИ) и хранятся носители ключевой информации, в том числе средства электронной подписи (далее – Спецпомещения).

1.4. Настоящий Порядок разработан в соответствии с:

Федеральным законом Российской Федерации от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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»;

приказом Федеральной службой безопасности России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.5. В каждом структурном подразделении департамента назначается ответственное лицо за доступ в Помещения.

1.6. Сотрудники департамента, допущенные в помещения, обязаны:
выполнять требования обеспечения безопасности Информации;
соблюдать режим конфиденциальности при обращении с Информацией, носителями Информации и СКЗИ (в том числе ключевыми документами к ним);

своевременно выявлять попытки посторонних лиц получить сведения об Информации, об используемых СКЗИ или ключевых документах к ним;

предусматривать отдельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

2. Общие требования к оборудованию помещений и регламентации доступа в них

2.1. Режим обеспечения безопасности помещений, в которых осуществляется обработка Информации (далее – Помещения) должен быть организован таким образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2.2. Ограждающие конструкции Помещений, должны предполагать существенные трудности для нарушителя по их преодолению (например, металлические решётки на окнах, металлическая дверь, система контроля и управления доступом и так далее).

2.3. Помещения должны быть оснащены надёжными входными дверьми с замками, а также средствами опечатывания помещений по окончании рабочего дня.

2.4. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

2.5. В департаменте определяется перечень помещений, в которых разрешена обработка Информации. Форма перечня представлена в приложении 1.

2.6. Доступ сотрудников в Помещения департамента должен быть организован согласно перечня лиц, допущенных в Помещения обработки Информации (форма перечня представлена в приложении 2). Перечень сотрудников, доступ которых разрешён в Помещения, размещается на внутренней стороне двери этого помещения.

2.7. В Помещениях определяются места хранения материальных носителей Информации и лиц, ответственных за их сохранность (форма перечня представлена в приложении 3).

2.8. Указанные перечни разрабатываются ответственными за доступ в Помещения лицами и утверждаются заместителем руководителя департамента, курирующего данное направление.

2.9. Доступ посторонних лиц в Помещения, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица из числа сотрудников, допущенных в Помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с защищаемой Информацией. Такими мерами являются: размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации; размещение документации на бумажных носителях, содержащих Информацию, исключающее просмотр Информации на них (документация убирается в папки, ящики тумбочек/столов, либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

2.10. В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведётся обработка Информации, должны быть надёжно закрыты, материальные носители должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

2.11. При необходимости повышенного уровня обеспечения безопасности Помещений могут использоваться системы видеонаблюдения и системы контроля и управления доступом.

3. Особенности доступа в серверные помещения

Доступ в серверные помещения посторонних лиц разрешается по согласованию с главным консультантом отдела кадровой работы, противодействия коррупции, учета и материально –технического обеспечения Л.В. Голиков.

3.1. Учёт доступа в серверные помещения третьих лиц (осуществляющих обслуживание, техническое сопровождение, настройку серверного и активного сетевого оборудования) должен отражаться в Журнале доступа в серверные помещения (форма журнала приведена в приложении 4 к настоящим Правилам).

3.2. Двери серверных помещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.

3.3. Уборка серверных помещений должна происходить только под контролем сопровождающего лица из числа сотрудников, допущенных в Помещение.

3.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

3.5. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за доступ в Помещения лицом.

3.6. Сотрудники органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – МЧС), аварийных служб, врачи «скорой помощи» допускаются в серверные помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении сотрудника, допущенного в Помещение.

4. Особенности доступа в спецпомещения

4.1. Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время.

4.2. Расположение Спецпомещений, специальное оборудование и организация режима в Спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.3. Двери Спецпомещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.

4.4. При утрате ключа от входной двери в Спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей (с документальным оформлением).

4.5. Доступ сотрудников в Спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов).

4.6. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в Спецпомещения иных лиц из числа сотрудников органов Департамента.

4.7. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя Подразделения или замещающего его лица.

4.8. Нахождение в Спецпомещениях посторонних лиц в нерабочее время запрещается.

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

Приложение 2
к Правилам доступа в помещения
департамента финансово-бюджетного
надзора Краснодарского края, в
которых ведётся обработка
защищаемой информации, в том числе
персональных данных

ФОРМА

ПЕРЕЧНЬ
лиц, допущенных в помещения обработки конфиденциальной
информации (в том числе персональных данных)

№ п/п	Наименование структурного подразделения	№ кабинета	Ф.И.О. сотрудника	Должность

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

Приложение 3
к Правилам доступа в помещения
департамента финансово-бюджетного
надзора Краснодарского края, в
которых ведётся обработка
защищаемой информации, в том числе
персональных данных

ФОРМА

ПЕРЕЧЕНЬ

**мест хранения материальных носителей конфиденциальной
информаций (в том числе персональных данных) и лиц,
ответственных за их сохранность**

№ п/п	Наименование структурного подразделения	Место хранения (номер помещения, № сейфа/шкафа)	Ответственное лицо (ФИО, должность)	Подпись

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения


Л.В. Голиков

Приложение 4

к правилам доступа в помещения
департамента финансово-
бюджетного надзора Краснодарского
края, в которых ведётся обработка
защищаемой информации, в том
числе персональных данных

ФОРМА

ЖУРНАЛ

доступа в серверное помещение департамента финансово-бюджетного
надзора Краснодарского края, размещенное по адресу: 350038, г.
Краснодар, ул. Короленко, д. 2/1, 1 этаж, помещение №113

№ п/п	Номер помещения	Название организации (проводящей работы) Ф.И.О. и должность сотрудника	Перечень проводимых работ и оборудования, к которому осуществляется доступ	Основание проводимых работ	Дата и время		Ф.И.О. должность сотрудника, сопровождающего третье лицо	Подпись
					начала работ	завершения работ		
1	2	3	4	5	6	7	8	9

Главный консультант отдела кадровой работы,
противодействия коррупции, учета и материально-технического
обеспечения


Л.В. Голиков

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в департаменте
финансово-бюджетного надзора Краснодарского края

1. Перечень персональных данных обрабатываемых в департаменте.

1.1. Перечень персональных данных:

- Фамилия, имя, отчество;
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве;
- место жительства (адрес регистрации, фактического проживания) и адреса прежних мест жительства;
- место жительства (адрес регистрации), почтовый адрес;
- серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- сведения о воинском учете и информация, содержащаяся в документах воинского учета;
- информация о наличии судимости (когда и за что);
- сведения о выполняемой работе с начала трудовой деятельности;
- место работы, должность;
- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера государственного гражданского служащего;
- сведения о доходах, расходах, имуществе и обязательствах имущественного характера, супруга (супруги) и несовершеннолетних детей;
- номер телефона (либо иной вид связи);
- информация о государственных наградах, иных наградах и знаках отличия (кем и когда награжден);
- сведения об инвалидности;
- сведения о судимости;
- ИНН, НДСЛ, документ подтверждающий регистрацию в системе

индивидуального (персонифицированного) учета;

сведения об отпусках;

сведения о начислении/удержании денежных средств;

сведения о временной нетрудоспособности;

классный чин государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы (кем и когда присвоены);

степень родства, фамилия, имя, отчество, дата рождения близких родственников (отец, мать, брат, сестра, ребенок), а также супруга (супруги)

место рождения, место работы (службы) и домашний адрес близких родственников (отца, матери, братьев, сестер и детей), а также супруга (супруги), в том числе бывших;

пребывание за границей (когда, где, с какой целью);

близкие родственники (отец, мать, братья, сестры и дети), а также супруг (супруга), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);

паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);

допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);

сведения согласно пунктов 2, 4 части 1 статьи 16 Федерального закона «О государственной гражданской службе в Российской Федерации».

1.2. Целями обработки перечисленных персональных данных являются:

обеспечения кадровой работы, в том числе в целях содействия гражданскими служащими в прохождении государственной гражданской службы, содействия в выполнении осуществляемой работы;

содействия гражданам в трудоустройстве (для граждан, претендующих на замещение вакантных должностей государственной гражданской службы в департаменте);

формирования кадрового резерва государственной гражданской службы;

профессионального развития и должностного роста;

учёта результатов исполнения государственными гражданскими служащими должностных обязанностей;

обеспечения личной безопасности государственных гражданских служащих и членов их семей;

обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества и имущества департамента;

заключение государственных контрактов и договоров.

рассмотрения устных и письменных обращений граждан по вопросам, относящимся к компетенции Департамента, с последующим уведомлением

граждан о результатах рассмотрения, и в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

Приложение 6
к приказу департамента
финансово-бюджетного
надзора
Краснодарского края
от _____ № _____

ПЕРЕЧЕНЬ

должностей департамента финансово-бюджетного надзора Краснодарского края, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Наименование структурного подразделения и должности государственной гражданской службы департамента финансово-бюджетного надзора Краснодарского края
1	2
1	Руководитель департамента финансово-бюджетного надзора Краснодарского края
2	Заместитель руководителя департамента финансово-бюджетного надзора Краснодарского края
3	Начальник отдела
4	Заместитель начальника отдела
5	Главный консультант
6	Консультант
7	Ведущий консультант
8	Главный специалист-эксперт
9	Главный государственный инспектор

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

ПЕРЕЧЕНЬ
информационных ресурсов и систем департамента
финансово-бюджетного надзора Краснодарского края, а
также сведений, обрабатываемых в них

1. Перечень информационных систем и ресурсов

1.1. Совокупность информационных ресурсов, доступ к которым осуществляется в департаменте финансово-бюджетного надзора Краснодарского края (далее – Департаменте), образуют информационную систему департамента финансово-бюджетного надзора Краснодарского края.

1.2. Перечень информационных систем:

№ п/п	Наименование ИС	Назначение ИС	Оператор ИС
1	2	3	4
1	ИС «ИС: Бухгалтерия»	Автоматизация финансовой детальности распорядителя и получателя бюджетных средств и выполнения функциональных обязанностей в рамках учетно-финансовой политики Департамента	Департамент финансово-бюджетного надзора Краснодарского края
2	ИС «ИС: Зарплата и кадры»	Автоматизация кадрового учета и начисления заработной платы сотрудников Департамента	Департамент финансово-бюджетного надзора Краснодарского края
3	ФГИС «Госслужба»	Формирование и использования базы данных открытых вакантных должностей государственной гражданской службы	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
4	ГИС «Электронный бюджет»	Обеспечение прозрачности, открытости, и подотчётности деятельности государственных органов и повышения качества их финансового управления	Федеральное казначейство Российской Федерации, Министерство финансов Российской Федерации
5	ЕМСЭД КК	Ведение делопроизводства в электронном виде различными	Департамент информатизации и

1	2	3	4
		подразделениям и исполнителями Департамента	связи Краснодарского края
6	АС «УРМ»	Автоматизация финансовой деятельности распорядителей и получателей бюджетных средств и организации электронного взаимодействия с Министерством финансов Краснодарского края	Министерство финансов Краснодарского края
7	СУФД	Управление платежами и финансовыми документами, формирование отчетности в автоматизированной системе Федерального казначейства	Управление федерального казначейства по Краснодарскому краю
8	АС «Web-Консолидация»	Сбор, контроль, консолидация и анализ отчетности в едином информационном пространстве с использованием WEB-технологий	Министерство финансов Краснодарского края
9	ГИС ГМП	Учет начислений фактов оплаты физическими и юридическими лицами государственных пошлин, денежных платежей и сборов.	Федеральное казначейство
10	РИССЗ КК	Обеспечение государственных и муниципальных нужд и обеспечение передачи и размещения в единой информационной системе информации и документов	Департамент по регулированию контрактной системы Краснодарского края
11	ИС «ССТУ»	Единый портал обработки обращений граждан Российской Федерации	Администрация Президента Российской Федерации
12	СЭД «Обращения граждан»	Автоматизация обработки обращений граждан РФ в Департамент	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Администрация Краснодарского края
13	ПК «Web-планирование»	Программный комплекс предназначен для комплексной автоматизации процессов планирования бюджета Департамента	Министерство финансов Краснодарского края
14	ФГИС «Закупки»	Автоматизация процессов в сфере закупок	Федеральное казначейство
15	ИС «СББОЛ»	Передача сведений в банковскую организацию о зачислении финансовых средств Департамента на личные счета сотрудников	ПАО «Сбербанк»
16	ИС «Контур - экстерн»	Предоставление отчетности Департаментом в электронном виде в контролирующие органы Российской Федерации	Контролирующие органы Российской Федерации

1	2	3	4
		Федерации	
17	ГЭС «Мой Арбитр»	Сервис предназначен для подачи документов в арбитражные суды Российской Федерации в электронном виде, посредством заполнения форм, размещенных на официальном сайте арбитражного суда	Федеральные арбитражные суды Российской Федерации
18	ГИС в области гражданской службы Краснодарского края	Автоматизация кадрового учета сотрудников Департамента	Департамент информатизации и связи Краснодарского края

2. Сведения о составе информации, обрабатываемой информационными ресурсами

№ п/п	Наименование ИР	Категория обрабатываемой информации	
		служебная информация	персональные данные
1	2	3	4
1	ИС «1С: Бухгалтерия»		
2	ИС «1С: Зарплата и кадры»		
3	ФГИС «Госслужба»		
4	ГИС «Электронный бюджет»		
5	ЕМСЭД КК		
6	АС «УРМ»		
7	СУФД		
8	АС «Web-Консолидация»		
9	ГИС ГМП		
10	ПК «РКС»		
11	ИС «ССТУ»		
12	СЭД «Обращения граждан»		
13	ПК «Web-планирование»		
14	ФГИС «Закупки»		
15	ИС «СББОЛ»		
16	ИС «Контур - экстерн»		
17	ГЭС «Мой Арбитр»		
18	ГИС в области гражданской службы Краснодарского края		

4. Структурные подразделения Департамента, имеющие доступ к информационным ресурсам

№ п/п	Наименование подразделения	ИС																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
1	2																					
1.	Руководство																					
2.	Отдел контроля в сфере закупок																					
3.	Отдел финансового контроля																					
4.	Отдел контроля в сфере межбюджетных отношений																					
5.	Отдел кадровой работы, противодействия коррупции, учета и материально-технического обеспечения																					
6.	Отдел организационно-правовой работы																					

Главный консультант отдела кадровой работы,
противодействия коррупции, учета
и материально-технического обеспечения



Л.В. Голиков

ОЦЕНКА
вреда, который может быть причинён субъектам
персональных данных департамента финансово-бюджетного
надзора Краснодарского края

1. Общие положения

1.1. Настоящий документ содержит оценку вреда, который может быть причинён субъектам персональных данных, (далее – Оценка возможного вреда), обрабатываемых в департаменте финансово-бюджетного надзора Краснодарского края (далее – департамент). Методику проведения оценки возможного вреда, а также соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

1.2. Оценка возможного вреда осуществляется в соответствии с требованиями статьи 18.1 Федерального закона «О персональных данных».

1.3. В связи с отсутствием нормативных документов Правительства Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации по Оценке возможного вреда субъектам персональных данных, производится качественная Оценка возможного вреда по методике, описанной в разделе 3 настоящего документа.

2. Термины и определения

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

2.2. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья,

интимной жизни субъектов персональных данных.

2.3. Биометрические персональные данные – персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (за исключением сведений, относящихся к специальным категориям персональных данных).

2.4. Общедоступные персональные данные – персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьёй 8 Федерального закона «О персональных данных».

2.5. Иные персональные данные – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных), за исключением персональных данных, относящихся к специальным, биометрическим или общедоступным персональным данным.

2.6. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.7. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

2.8. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

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

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

2.11. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

2.12. Целостность информации – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

2.13. Доступность информации – состояние информации (ресурсов информационной системы), при которой субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

3. Методики Оценки возможного вреда

3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения характеристик безопасности информации (персональных данных):

3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.

3.2.2. Неправомерное блокирование персональных данных является нарушением доступности персональных данных.

3.2.3. Неправомерное уничтожение персональных данных является нарушением доступности и целостности персональных данных.

3.2.4. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

3.2.5. Нарушение права субъекта персональных данных требовать от оператора персональных данных уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации.

3.2.6. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.

3.2.7. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

3.2.8. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинён вред в форме:

3.3.1. Морального вреда – физические или нравственные страдания, причинённые субъекту персональных данных, действиями (или бездействием) оператора персональных данных, нарушающими личные неимущественные права субъекта персональных данных, либо посягающими на принадлежащие субъекту персональных данных нематериальные блага, а также в других случаях, предусмотренных законом.

3.3.2. Убытков – расходы, которые лицо (субъект персональных данных), чьё право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было

нарушено (упущенная выгода).

3.4. Оценка возможного вреда субъектам персональных данных определяется в соответствии следующими качественными критериями оценки нарушения заданных характеристик безопасности персональных данных:

3.4.1. Высокий – приводит к значительным негативным последствиям для субъекта персональных данных, а именно:

нанесение крупного ущерба субъекту персональных данных;

крупные финансовые потери для субъекта персональных данных в результате неправомерных действий с персональными данными;

возможно нанесение тяжелого вреда здоровью субъекта или возможность реализации прямой угрозы жизни.

3.4.2. Средний – приводит к негативным последствиям для субъекта персональных данных, а именно:

причинение ущерба субъекту персональных данных;

значительные финансовые потери в результате неправомерных действий с персональными данными;

возможно нанесение вреда, не создающего угрозы жизни или здоровью субъекту персональных данных.

3.4.3. Низкий – приводит к незначительным последствиям для субъекта персональных данных, а именно:

нанесение незначительного ущерба субъекту персональных данных или отсутствие подобного вреда;

отсутствие финансовых потерь или незначительные потери для субъекта персональных данных;

отсутствие вреда здоровью или жизни субъекту персональных данных, или незначительный вред.

4. Оценка возможного вреда

4.1. Степень возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяется по наибольшему значению возможного нарушения каждой из характеристик безопасности информации и отношении категорий субъектов персональных данных, чьи персональные данные обрабатываются в департаменте.

4.2. Оценка возможного вреда приведена в приложении 1 к настоящему документу.

4.3. Для всех категорий субъектов персональных данных, чьи персональные данные обрабатываются в департаменте, определена средняя степень возможного ущерба, так как:

в составе персональных данных, обрабатываемых в департаменте, отсутствуют сведения, неправомерные действия с которыми, могут привести к причинению крупного вреда субъекту персональных данных;

угроза нанесения тяжкого вреда здоровью или угроза жизни и здоровью субъектам персональных данных отсутствует.

5. Соотношение возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

5.1. В департаменте принимаются правовые, организационные и технические меры, необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

5.2. Состав мер, направленных на защиту персональных данных, определяется исходя из требований, установленных:

Федеральным законом Российской Федерации «О персональных данных».

Федеральным законом Российской Федерации от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»;

Федеральным законом Российской Федерации от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

Федеральным законом Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

Указом Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

приказом Федеральной службы по техническому и экспертному контролю Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказом Федеральной службы по техническому и экспертному контролю Российской Федерации России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5.3. Соотношение возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приведено в приложении 2 к настоящему документу.

Главный консультант
отдела кадровой работы,
противодействия коррупции, учета и
материально-технического обеспечения



Л.В. Голиков

Приложение 1
к оценке вреда, который может быть
причинён субъектам персональных данных
департамента финансово-бюджетного
надзора Краснодарского края

**ОЦЕНКА
возможного вреда**

№ п/п	Категория субъектов персональных данных	Категория персональных данных	Характеристика безопасности информации	Степень возможного вреда	Примечание
1	2	3	4	5	6
1	сотрудники департамента	Общедоступные	Конфиденциальность		Нарушение конфиденциальности общедоступных персональных данных не несёт за собой вред субъектам
			Целостность	Низкая	
			Доступность	Низкая	
		Биометрические	Конфиденциальность	Средняя	
			Целостность	Низкая	
			Доступность	Низкая	
		Специальные	Конфиденциальность	Средняя	
			Целостность	Средняя	
		Иные	Доступность	Низкая	
			Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	
2	граждане, претендующие на замещение вакантных должностей государственной гражданской службы	Общедоступные	Конфиденциальность		Данная категория персональных данных не обрабатывается
			Целостность		
			Доступность		
		Биометрические	Конфиденциальность	Средняя	
			Целостность	Низкая	
			Доступность	Низкая	

1	2	3	4	5	6
		Специальные	Конфиденциальность	Средняя	
		Иные	Целостность	Средняя	
			Доступность	Низкая	
		Общедоступные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	
3	Граждане, обратившиеся в Министерство в порядке, предусмотренном Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»	Биометрические	Конфиденциальность		Данные категории персональных данных не обрабатываются
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	

Главный консультант
отдела кадровой работы,
противодействия коррупции, учета и
материально-технического обеспечения



Л.В. Голиков

Приложение 2
к оценке вреда, который может
быть причинён субъектам
персональных данных субъектам
персональных данных департамента
финансово-бюджетного надзора
Краснодарского края

СООТНОШЕНИЕ

**возможного вреда и принимаемых оператором мер, направленных на
обеспечение выполнения обязанностей, предусмотренных Федеральным
законом «О персональных данных»**

№ п/п	Перечень мер, принимаемых для обеспечения защиты персональных данных	Степень возможного вреда субъекту персональных данных, при невыполнении меры
1	2	3
1	Сбор согласий на обработку персональных данных, в случаях, установленных Федеральным законом «О персональных данных»	Средняя
2	Оценка вреда субъектам персональных данных	Средняя
3	Обезличивание, уточнение и уничтожение персональных данных, в случаях, когда это необходимо	Средняя
4	Определение правил рассмотрения запросов субъектов персональных данных или их представителей	Средняя
5	Определение правил работы с обезличенными данными в случае обезличивания персональных данных	Средняя
6	Определение порядка доступа в помещения Департамент, в которых ведётся обработка персональных данных	Средняя
7	Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Департамент	Средняя
8	Определение угроз безопасности персональных данных, при их обработке в информационных системах Департамент	Средняя
9	Определение уровня защищённости персональных данных, обрабатываемых в информационных системах Департамент	Средняя
10	Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Департамент, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных	Средняя
11	Исключение несанкционированного, в том числе случайного,	Средняя

1	2	3
	доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных	
12	Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации	Средняя
13	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных	Средняя
14	Учёт машинных носителей персональных данных	Средняя
15	Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер	Средняя
16	Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Средняя
17	Установление правил доступа к персональным данным, а также обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационных системах Департамент	Средняя
18	Контроль за принимаемыми мерами по обеспечению безопасности персональных данных	Средняя

Главный консультант
отдела кадровой работы,
противодействия коррупции, учета и
материально-технического обеспечения



Л.В. Голиков

Приложение 9
к приказу департамента
финансово-бюджетного
надзора
Краснодарского края
от 24.11.2020 № 145

ФОРМА

Руководителю департамента финансово-
бюджетного надзора Краснодарского края

Ф.И.О. субъекта персональных данных

номер основного документа, удостоверяющего личность

наименование выдавшего органа

дата выдачи

СОГЛАСИЕ на обработку персональных данных

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
проживающий по адресу: _____,
в _____
(адрес субъекта персональных данных)
соответствии с Федеральным законом от 27 июля 2007 года №152-ФЗ «О
персональных данных» даю своё согласие департаменту финансово-
бюджетного надзора Краснодарского края (далее – Оператор),
расположенному по адресу: г. Краснодар, ул. Короленко, д.2\1, на обработку,
как с использованием средств автоматизации, так и без использования таких
средств, включая (сбор, запись, систематизацию, накопление, хранение,
уточнение, извлечение, использование, передачу, обезличивание,
блокирование, удаление, уничтожение) следующих моих персональных
данных: _____,
полученных Оператором в результате вступления со мной в правоотношения с
целью оказания мне услуг Оператором, обеспечения соблюдения требований
законов и иных нормативно-правовых актов, а также предоставления
сторонним лицам (включая органы государственного и муниципального

управления, а также банкам) в рамках исполнения требований законодательства Российской Федерации.

Обработка персональных данных разрешается на период наличия указанных выше правоотношений, а также на срок, установленный нормативно-правовыми актами Российской Федерации.

Срок действия согласия – бессрочно, до момента его отзыва.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Подтверждаю ознакомление с «Правилами обработки персональных данных в департаменте финансово-бюджетного надзора Краснодарского края », правами и обязанностями в области защиты персональных данных.

Субъект персональных данных: _____ / _____
(подпись) (ФИО)

Дата: «__» _____ 20__ г.

Приложение 10
к приказу департамента
финансово-бюджетного
надзора
Краснодарского края
от 24.11.2020 № 145

ФОРМА

**Разъяснение субъекту персональных данных
(замещающему должность государственной гражданской
службы в департаменте финансово-бюджетного надзора
Краснодарского края) юридических последствий отказа
предоставить свои персональные данные**

В соответствии со статьями 26, 42 Федерального закона от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утверждённого Указом Президента Российской Федерации от 30 мая 2005 года № 609, определён перечень персональных данных, которые субъект персональных данных обязан предоставить департамент финансово-бюджетного надзора Краснодарского края в связи с поступлением или прохождением государственной гражданской службы.

Без представления субъектом персональных данных, обязательных для заключения служебного контракта сведений, служебный контракт не может быть заключён.

На основании пункта 11 части 1 статьи 33 Федерального закона от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» служебный контракт прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности государственной гражданской службы.

Мне, _____,
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные департаменту финансово-бюджетного надзора Краснодарского края.

_____ дата

_____ подпись

_____ расшифровка подписи

Приложение 11
к приказу департамента
финансово-бюджетного
надзора
Краснодарского края
от 24.11.2020 № 145

ФОРМА

Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

В соответствии с принципами обработки персональных данных, установленными Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, и актуальность по отношению к заявленным целям обработки персональных данных.

Кроме того, оператор должен принимать необходимые меры по уточнению неполных или неточных персональных данных.

В случае, если субъект персональных данных отказывается предоставить свои персональные данные, либо представленные персональные данные являются неточными и (или) неполными по отношению к заявленным целям обработки персональных данных, департамент финансово-бюджетного надзора Краснодарского края оставляет за собой право отказать в предоставлении своих услуг субъекту персональных данных.

Мне, _____
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные департамента финансово-бюджетного надзора Краснодарского края.

_____ дата

_____ подпись

_____ расшифровка подписи

Приложение 12
к приказу департамента
финансово-бюджетного
надзора
Краснодарского края
от 24.11.2020 № 145

ФОРМА

ОБЯЗАТЕЛЬСТВО
сотрудника департамента финансово-бюджетного надзора
Краснодарского края, непосредственно осуществляющего
обработку персональных данных

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

обязуюсь:

знать и выполнять требования законодательства в области персональных данных;

хранить в тайне известные мне персональные данные, информировать лицо, ответственное за организацию обработки персональных данных в министерстве, о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей;

прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной государственного контракта, освобождения меня от замещаемой должности и увольнения с государственной гражданской службы.

В соответствии со статьёй 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются информацией ограниченного доступа, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная законодательством Российской Федерации, за разглашение информации ограниченного доступа, мне разъяснена.

_____ дата

_____ подпись

_____ расшифровка подписи