АДМИНИСТРАЦИЯ АЛТАЙСКОГО КРАЯ

ГЛАВНОЕ УПРАВЛЕНИЕ СТРОИТЕЛЬСТВА, ТРАНСПОРТА, ЖИЛИЩНО-КОММУНАЛЬНОГО И ДОРОЖНОГО ХОЗЯЙСТВА АЛТАЙСКОГО КРАЯ

ПРИКАЗ

«01» 03 2016 г. № 57

г. Барнаул

О мерах по обеспечению безопасности персональных данных

В целях соблюдения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» п р и к а з ы в а ю:

1. Назначить ответственным за организацию обработки и обеспечение безопасности персональных данных в Главном управлении начальника отдела программных средств и технологий Степанищева Алексея Владимировича.

2. Возложить на отдел программных средств и технологий функции по администрированию безопасности информационных систем персональных данных.

3. Утвердить:

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края;

Инструкцию ответственного за организацию обработки и обеспечение безопасности персональных данных Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края.

4. Ознакомить с данным приказом гражданских служащих и сотрудников Главного управления, имеющих доступ к персональным данным.

5. Признать утратившим силу приказ Главного управления от 18.09.2015 № 787 «О мерах по обеспечению безопасности персональных данных».

6. Контроль за исполнением настоящего приказа возложить на заместителя начальника Главного управления, начальника управления экономического планирования, мониторинга и контроля Гилева И.В.

Заместитель начальника
Главного управления И.В. Гилев

УТВЕРЖДЕНО
приказом Главного управления
№ 57 от 01.03.2016

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Главного управления (далее – «Положение») разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Главного управления (далее - «оператор персональных данных»).

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается применением организационных мер и технических средств защиты информации (в том числе средств предотвращения несанкционированного доступа). Организационные меры и технические средства защиты информации должны удовлетворять требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.4. Требования настоящего Положения являются обязательными для исполнения всеми лицами, получившими доступ к персональным данным.

1.5. Решение о необходимости изменения этого Положения принимается на основании:

результатов проведенных аудитов, мероприятий по контролю и надзору за обеспечением безопасности персональных данных, осуществляемых уполномоченными органами;

изменения нормативных правовых актов и (или) нормативных методических документов Российской Федерации в области защиты

персональных данных;

изменения процессов обработки персональных данных в информационных системах (далее – «ИС») персональных данных Главного управления;

результатов анализа инцидентов информационной безопасности в ИС персональных данных.

Изменения Положения должны быть направлены на предотвращение инцидентов или устранение последствий уже реализованных инцидентов информационной безопасности.

Все предлагаемые изменения Положения подлежат предварительной оценке до их ввода в действие на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2. Обработка персональных данных

2.1. Оператор персональных данных осуществляет обработку персональных данных лиц, замещающих должности государственной гражданской службы Алтайского края, и должности, не относящиеся к должностям государственной гражданской службы Алтайского края, а также лиц, не являющихся сотрудниками оператора.

2.2. Обработка персональных данных осуществляется оператором персональных данных в целях реализации возложенных на него функций, определяемых законами и иными нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2.3. Объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки. Обрабатываемые персональные данные должны соответствовать заявленным целям обработки. Недопустимо объединение созданных для несовместимых между собой целей баз данных ИС персональных данных.

2.4. Обработка персональных данных осуществляется оператором без проведения мероприятий по обезличиванию персональных данных.

2.5. Персональные данные оператор получает непосредственно от субъектов персональных данных, которые принимают решение об их предоставлении и дают согласие на их обработку своей волей и в своем интересе.

2.6. Лица, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списков сотрудников, допущенных к соответствующим персональным данным.

2.7. Принятые в Главном управлении организационно-распорядительные документы доводятся до сведения лиц, участвующих в

процессе обработке персональных данных в части их касающейся.

2.8. Персональные данные, используемые для обработки в ИС, порядок их использования, цель, периодичность и основания внесения изменений и дополнений в организационные документы, а также порядок хранения персональных данных устанавливаются оператором персональных данных.

2.9. Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

2.10. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению по достижении всех целей их обработки или в случае утраты необходимости в достижении этих целей. Оператор по согласованию с субъектом персональных данных может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора законодательством Российской Федерации.

3. Обязанности и права оператора персональных данных в ИС

3.1. Оператор персональных данных обязан предоставлять субъекту персональных данных возможность ознакомления с его персональными данными, а также вносить в них необходимые изменения, уничтожать или блокировать соответствующие персональные данные в случае предоставления субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор в ИС персональных данных, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и принятых мерах оператор персональных данных уведомляет субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

3.2. В случае выявления недостоверных персональных данных или фактов неправомерных действий с ними оператора персональных данных при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.3. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом

персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких документов и снять блокирование персональных данных.

3.4. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.5. Оператор персональных данных в случае достижения всех целей обработки персональных данных обязан незамедлительно прекратить их обработку и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения всех целей обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами. По согласованию с субъектом персональных данных оператор может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора законодательством Российской Федерации.

3.6. Оператор персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных

данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3.7. Оператор при передаче персональных данных субъектов третьим лицам, только с согласия субъекта персональных данных, ограничивает передаваемую информацию только теми персональными данными субъектов, которые необходимы третьим лицам для выполнения своих функций. Передача персональных данных по телефону, факсимильной связи, электронной почте и сети Интернет (без использования средств защиты информации, удовлетворяющих требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных) запрещается.

4. Методы и способы защиты персональных данных в информационных системах персональных данных

4.1. С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, оператором должны быть установлены уровни защищенности персональных данных ИС.

4.2. В целях обеспечения безопасности персональных данных определяются угрозы безопасности, оценивается актуальность угроз безопасности персональных данных. В результате разрабатывается модель угроз безопасности персональных данных.

Модель угроз безопасности персональных данных корректируется при изменении состава основных технических средств и условий эксплуатации ИС персональных данных сотрудниками отдела программных средств и технологий Главного управления.

4.3. Установка, изменение (обновление) и удаление программного обеспечения в ИС персональных данных производится администратором безопасности ИС персональных данных или в его присутствии.

4.4. Доступ лиц к ИС персональных данных, не допущенных к работе с персональными данными, должен быть исключен. ИС персональных данных должны быть защищены аппаратными и (или) программными средствами защиты информации от несанкционированного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

4.5. Обработка персональных данных в ИС осуществляется с использованием средств защиты информации в соответствии с установленными требованиями нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности информации.

4.6. Охрана помещений, в которых ведется работа с персональными

данными, и организация режима безопасности в этих помещениях должна обеспечивать сохранность технических средств и носителей персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Все носители персональных данных должны быть учтены с помощью их маркировки, а их учетные данные занесены в журнал учета с отметкой об их выдаче (приеме).

4.7. В целях обеспечения безопасности персональных данных должны быть разработаны организационно-распорядительные и организационно-методические документы по обеспечению безопасности персональных данных, обрабатываемых в ИС:

перечень информационных систем персональных данных Главного управления – Приложение №1;

перечень персональных данных, обрабатываемых в Главном управлении в связи с реализацией служебных (трудовых) отношений – Приложение №2;

перечень должностей сотрудников Главного управления, допущенных к соответствующим персональным данным – Приложение №3;

порядок доступа сотрудников Главного управления в помещения, в которых ведется обработка персональных данных – Приложение №4;

инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных – Приложение №5;

инструкция по правилам обращения с носителями ключевой информации в информационных системах Главного управления – Приложение №6;

правила рассмотрения запросов субъектов персональных данных или их представителей в Главное управление – Приложение №7;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Главном управлении – Приложение №8;

правила обработки персональных данных в Главном управлении – Приложение №9;

другие организационно-распорядительные документы по обеспечению безопасности персональных данных, обрабатываемых в информационных системах.

4.8. Лица, уполномоченные осуществлять обработку персональных данных, несут ответственность за соблюдение требований по защите персональных данных в порядке, предусмотренном действующим законодательством Российской Федерации.

5. Обязанности и права должностных лиц

5.1. Начальник Главного управления:

организует разработку, внедрение, совершенствование и эксплуатацию системы защиты ИС персональных данных, а также организует внутренний

контроль за соблюдением нормативных правовых актов Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

осуществляет финансовое, материально-техническое и иное обеспечение мероприятий по защите персональных данных при их обработке в ИС персональных данных Главного управления;

назначает ответственного за организацию обработки персональных данных;

назначает ответственного за обеспечение безопасности персональных данных;

назначает администратора безопасности ИС персональных данных.

5.2. Ответственный за организацию обработки персональных данных:

осуществляет внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводит до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

организует и осуществляет прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

5.3. Ответственный за обеспечение безопасности персональных данных:

несет ответственность за организацию обеспечения безопасности персональных данных при их обработке в ИС Главного управления;

обеспечивает выполнение организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных;

организует расследование причин и условий появления нарушений безопасности ИС персональных данных, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений.

5.4. Администратор безопасности ИС персональных данных:

обеспечивает обнаружение фактов несанкционированного доступа к ИС персональных данных, о которых должен доложить ответственному за обеспечение безопасности персональных данных;

осуществляет установку и ввод в эксплуатацию средств защиты информации ИС персональных данных в соответствии с эксплуатационной и технической документацией;

обеспечивает работы по проведению антивирусного контроля в ИС персональных данных;

выполняет резервное копирование персональных данных;

осуществляет установку (обновление версий) программного обеспечения ИС персональных данных, обеспечивает его функционирование;

осуществляет установку, подключение и настройку технических средств ИС персональных данных в соответствии с технической

документацией;

осуществляет установку (развертывание) новых ИС персональных данных или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач;

организует регистрацию и осуществляет учет защищаемых носителей информации.

5.5. Отдел программных средств и технологий Главного управления:

организует выполнение мероприятий по защите персональных данных при их обработке в ИС персональных данных;

обеспечивает обслуживание и ремонт сетевого оборудования, рабочих станций, серверного и периферийного оборудования в ИС персональных данных.

6. Контроль состояния защиты персональных данных

6.1. Контроль и надзор за соответствием обработки персональных данных осуществляется уполномоченным органом по защите прав субъектов персональных данных, которым является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

6.2. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных, осуществляется ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных.

7. Заключительные положения

7.1. Настоящее Положение вступает в силу с момента его утверждения.

7.2. Настоящее Положение не заменяет собой действующее законодательство Российской Федерации, регулирующее отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

Приложение № 1
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ПЕРЕЧЕНЬ
информационных систем персональных данных
Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

В Главном управлении обрабатываются персональные данные в следующих информационных системах персональных данных (далее – «ИСПДн»):

ИСПДн «1С: Предприятие 8.2 Бухгалтерия предприятия (архивная)», с 4 уровнем защищенности;

ИСПДн «1С: Предприятие 8.2 Зарплата и кадры», с 4 уровнем защищенности;

ИСПДн «1С: Предприятие 8.2 Бухгалтерия предприятия», с 4 уровнем защищенности;

ИСПДн «2НДФЛ (архивная)», с 4 уровнем защищенности;

ИСПДн «SPU_ORB (архивная)», с 4 уровнем защищенности;

ИСПДн «SPU_ORB», с 4 уровнем защищенности;

ИСПДн «Выдача разрешений на строительство, реконструкцию и ввод в эксплуатацию объектов капитального строительства в границах особо охраняемой природной территории краевого значения (за исключением лечебно-оздоровительных местностей и курортов), объектов капитального строительства на территориях двух и более муниципальных образований (муниципальных районов, городских округов), объектов, расположенных на территории особой экономической зоны», с 4 уровнем защищенности;

ИСПДн «Доверенности (word)», с 4 уровнем защищенности;

ИСПДн «Договоры с физическими лицами (word)», с 4 уровнем защищенности;

ИСПДн «Заявления граждан на выдачу разрешений на перевозку пассажиров и багаже легковым такси», с 4 уровнем защищенности;

ИСПДн «Контур-Экстерн (архивная)», с 4 уровнем защищенности;

ИСПДн «Обращения граждан (word, excel)», с 4 уровнем защищенности;

ИСПДн «Пофамильный перечень граждан, которых необходимо

переселить из аварийного жилищного фонда», с 4 уровнем защищенности;

ИСПДн «Реестр почтовых отправлений (word, excel)», с 4 уровнем защищенности;

ИСПДн «Сбербанк-онлайн», с 4 уровнем защищенности;

ИСПДн «СБИС++», с 4 уровнем защищенности;

ИСПДн «Списки сотрудников (word, excel)», с 4 уровнем защищенности;

ИСПДн «Списки умерших», с 4 уровнем защищенности;

ИСПДн «Фаст: Зарплата (архивная)», с 4 уровнем защищенности;

Приложение № 2
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в Главном управлении строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

В информационных системах персональных данных (далее – «ИСПДн») Главного управления обрабатываются следующие персональные данные:

1. ИСПДн «1С: Предприятие 8.2 Бухгалтерия предприятия (архивная)»
- фамилия, имя, отчество;
- адрес;
- паспортные данные;

2. ИСПДн «1С: Предприятие 8.2 Зарплата и кадры»
- фамилия, имя, отчество;
- СНИЛС;
- ИНН;
- адрес;
- паспортные данные;
- образование;
- страховой полис;
- состав семьи;

3. ИСПДн «1С: Предприятие 8.2 Бухгалтерия предприятия»
- фамилия, имя, отчество;
- адрес;
- паспортные данные;

4. ИСПДн «2НДФЛ (архивная)»
- фамилия, имя, отчество;
- СНИЛС;
- ИНН;

5. ИСПДн «SPU_ORB (архивная)»
- фамилия, имя, отчество;
- СНИЛС;
- ИНН;

6. ИСПДн «SPU_ORB»
- фамилия, имя, отчество;

- СНИЛС;
- ИНН;

7. ИСПДн «Выдача разрешений на строительство, реконструкцию и ввод в эксплуатацию объектов капитального строительства в границах особо охраняемой природной территории краевого значения (за исключением лечебно-оздоровительных местностей и курортов), объектов капитального строительства на территориях двух и более муниципальных образований (муниципальных районов, городских округов), объектов, расположенных на территории особой экономической зоны»

- фамилия, имя, отчество;
- паспортные данные;

8. ИСПДн «Доверенности (word)»

- фамилия, имя, отчество;
- адрес места проживания;
- номер паспорта;

9. ИСПДн «Договоры с физическими лицами (word)»

- фамилия, имя, отчество;
- адрес места проживания;
- номер паспорта;

10. ИСПДн «Заявления граждан на выдачу разрешений на перевозку пассажиров и багаже легковым такси»

- фамилия, имя, отчество;
- адрес места проживания;
- паспортные данные;

11. ИСПДн «Контур-Экстерн (архивная)»

- фамилия, имя, отчество;
- СНИЛС;
- ИНН;

12. ИСПДн «Обращения граждан (word, excel)»

- фамилия, имя, отчество;
- адрес места проживания;
- номер домашнего телефона;
- адрес электронной почты;
- номер мобильного телефона;

13. ИСПДн «Пофамильный перечень граждан, которых необходимо переселить из аварийного жилищного фонда»

- фамилия, имя, отчество;
- адрес места проживания;
- паспортные данные;

14. ИСПДн «Сбербанк-онлайн»

- фамилия, имя, отчество;
- номер р/с;
- сумма к перечислению;

15. ИСПДн «СБИС++»

- фамилия, имя, отчество;
- адрес места проживания;

- СНИЛС;
- ИНН;

16. ИСПДн «Списки сотрудников (word, excel)»
- фамилия, имя, отчество;
- адрес места проживания;
- паспортные данные;
- номер мобильного телефона;

17. ИСПДн «Списки умерших»
- фамилия, имя, отчество;
- дата рождения;
- дата смерти;
- место захоронения;

18. ИСПДн «Фаст: Зарплата (архивная)»
- фамилия, имя, отчество;
- СНИЛС;
- ИНН;
- адрес места проживания;
- номер паспорта;
- образование;
- страховой полис;
- состав семьи.

Приложение № 3
к Положению об обеспечении
безопасности персональных
данных при их обработке в
информационных системах
Главного управления
строительства, транспорта,
жилищно-коммунального и
дорожного хозяйства
Алтайского края

ПЕРЕЧЕНЬ

должностей сотрудников Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края, допущенных к соответствующим персональным данным

Наименование должности	Вид персональных данных	Степень доступа к персональным данным
Начальник отдела финансов и бухгалтерского учета – главный бухгалтер	Персональные данные гражданских служащих и работников Главного управления	Персональные данные, необходимые для начисления и выплаты денежного содержания и заработной платы, страховых взносов, оформления карточек для получения денежного содержания и заработной платы
Заместитель начальника отдела финансов и бухгалтерского учета	Персональные данные гражданских служащих и работников Главного управления	Персональные данные, необходимые для начисления и выплаты денежного содержания и заработной платы, страховых взносов, оформления карточек для получения денежного содержания и заработной платы
Консультант отдела финансов и бухгалтерского учета (2 сотрудника)	Персональные данные гражданских служащих и работников Главного управления	Персональные данные, необходимые для начисления и выплаты денежного содержания и заработной платы, страховых взносов, оформления карточек для получения денежного содержания и заработной платы
Главный специалист отдела финансов и бухгалтерского учета (5 сотрудников)	Персональные данные гражданских служащих и работников Главного управления	Персональные данные, необходимые для начисления и выплаты денежного содержания и заработной платы,

		страховых взносов, оформления карточек для получения денежного содержания и заработной платы
Главный специалист 11 разряда отдела финансов и бухгалтерского учета (2 сотрудника)	Персональные данные гражданских служащих и работников Главного управления	Персональные данные, необходимые для начисления и выплаты денежного содержания и заработной платы, страховых взносов, оформления карточек для получения денежного содержания и заработной платы
Начальник отдела по контролю за соблюдением законодательства о градостроительной деятельности	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для выдачи разрешений на строительство
Консультант отдела по контролю за соблюдением законодательства о градостроительной деятельности	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для выдачи разрешений на строительство
Главный специалист отдела по контролю за соблюдением законодательства о градостроительной деятельности	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для выдачи разрешений на строительство
Начальник юридического отдела	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в юридическом отделе Главного управления
Заместитель начальника юридического отдела	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в юридическом отделе Главного управления
Консультант юридического отдела (2 сотрудника)	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в юридическом отделе Главного управления
Главный специалист юридического отдела (2 сотрудника).	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в юридическом отделе Главного управления

Начальник отдела документационной и организационной работы	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе документационной и организационной работы Главного управления
Консультант отдела документационной и организационной работы	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе документационной и организационной работы Главного управления
Ведущий специалист отдела документационной и организационной работы (3 сотрудника)	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе документационной и организационной работы Главного управления
Начальник отдела мониторинга и контроля	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе мониторинга и контроля Главного управления
Заместитель начальника отдела мониторинга и контроля	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе мониторинга и контроля Главного управления
Консультант отдела мониторинга и контроля (2 сотрудника)	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе мониторинга и контроля Главного управления
Главный специалист отдела мониторинга и контроля (2 сотрудника)	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в отделе мониторинга и контроля Главного управления
Консультант претензионно-искового отдела (3 сотрудника)	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в претензионно-исковом отделе Главного управления
Главный специалист	Персональные данные	Персональные данные,

претензионно-искового отдела	гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	содержащиеся в документах, проходящих процедуру согласования в претензионно-исковом отделе Главного управления
Главный специалист 11 разряда претензионно-искового отдела	Персональные данные гражданских служащих и работников Главного управления, а так же граждан, с ним взаимодействующих	Персональные данные, содержащиеся в документах, проходящих процедуру согласования в претензионно-исковом отделе Главного управления
Начальник сектора жилищного строительства отдела строительства	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист сектора жилищного строительства отдела строительства (2 сотрудника)	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Начальник сектора строительства отдела строительства	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист отдела архитектуры и территориального планирования	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Начальник отдела промышленности строительных материалов	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист отдела промышленности строительных материалов	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Ведущий специалист отдела промышленности строительных материалов	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Начальник отдела по контролю за соблюдением законодательства о градостроительной деятельности	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Консультант отдела по контролю за соблюдением	Персональные данные граждан, взаимодействующих с	Персональные данные, содержащиеся в документах, необходимых

законодательства о градостроительной деятельности	Главным управлением	для обработки обращений граждан
Главный специалист отдела по контролю за соблюдением законодательства о градостроительной деятельности	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Ведущий специалист отдела по контролю за соблюдением законодательства о градостроительной деятельности	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Ведущий специалист отдела автотранспорта	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист 11 разряда сектора авиационного и речного транспорта отдела транспорта	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист отдела дорожного хозяйства	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист отдела теплоснабжения (2 сотрудника)	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Ведущий специалист отдела теплоснабжения	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Консультант отдела газификации	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист отдела водоснабжения (2 сотрудника)	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист 11 разряда отдела водоснабжения	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Начальник жилищного отдела	Персональные данные граждан,	Персональные данные, содержащиеся в

	взаимодействующих с Главным управлением	документах, необходимых для обработки обращений граждан
Консультант жилищного отдела	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист жилищного отдела (3 сотрудника)	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист 11 разряда жилищного отдела	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Старший инспектор (2 сотрудника)	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист отдела транспорта	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Главный специалист 11 разряда жилищного отдела.	Персональные данные граждан, взаимодействующих с Главным управлением	Персональные данные, содержащиеся в документах, необходимых для обработки обращений граждан
Начальник отдела спецработы и кадров	Персональные данные гражданских служащих и работников Главного управления, граждан, претендующих на замещение вакантной должности государственной гражданской службы	Все персональные данные, содержащиеся в личных делах гражданских служащих и работников Главного управления, включая персональные данные руководителя и заместителя руководителя Главного управления
Консультант отдела спецработы и кадров	Персональные данные гражданских служащих и работников Главного управления, граждан, претендующих на замещение вакантной должности государственной гражданской службы	Все персональные данные, содержащиеся в личных делах гражданских служащих и работников Главного управления, включая персональные данные руководителя и заместителя руководителя Главного управления

Приложение № 4
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ПОРЯДОК

доступа сотрудников Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края в помещения, в которых ведется обработка персональных данных

1. Общие положения

1.1. Порядок доступа сотрудников Главного управления в помещения, в которых ведется обработка персональных данных (далее - Порядок) устанавливает единые требования к доступу сотрудников Главного управления в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Главном управлении и обеспечения соблюдения требований законодательства о персональных данных.

1.2. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками Главного управления.

2. Требования к служебным помещениям

2.1. В целях обеспечения соблюдения требований к ограничению доступа в служебные помещения Главного управления обеспечивается:

использование служебных помещений строго по назначению;

наличие на входах в служебные помещения дверей, оборудованных запорными устройствами;

содержание дверей служебных помещений в нерабочее время в закрытом на запорное устройство;

остекление окон в зданиях Главного управления, содержание их в нерабочее время в закрытом состоянии.

2.2. Доступ в служебные помещения сотрудников допускается только для выполнения поручений и получения информации, необходимой для исполнения служебных обязанностей в соответствии с должностной инструкцией, иных лиц - в случаях, установленных законодательством.

2.3. Сотрудникам Главного управления запрещается передавать ключи от служебных помещений третьим лицам.

Приложение № 5
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ИНСТРУКЦИЯ

по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных

1. Общие положения

1.1. Настоящая Инструкция устанавливает требования к организации учета и использования машинных носителей информации, предназначенных для обработки и хранения персональных данных в информационных системах персональных данных (далее - ИСПДн).

1.2. Учет машинных носителей информации, предназначенных для обработки и хранения персональных данных, осуществляет ответственный за организацию обработки персональных данных.

1.3. Все машинные носители информации, предназначенные для обработки и хранения персональных данных (далее - МНИ) регистрируются по журналу учета и выдачи машинных носителей информации, содержащих персональные данные (далее - Журнал) ответственным за организацию обработки персональных данных.

1.4. Ответственность за сохранность полученных МНИ несет пользователь ИСПДн.

2. Учет машинных носителей информации, предназначенных для обработки и хранения персональных данных

2.1. К МНИ относятся:

съемные носители информации;

несъемные носители информации.

2.2. При обработке персональных данных на ПЭВМ соблюдается следующий порядок учета, хранения МНИ:

2.2.1. Каждому МНИ присваивается учетный номер по Журналу. Учетный номер наносится на МНИ ответственным за организацию обработки персональных данных. Если невозможно маркировать непосредственно МНИ, то маркируется упаковка, в которой он хранится.

Учетный номер состоит из двух частей АААХХХ, где

ААА - буквенное сокращение из 3 символов (определяются ответственным за организацию обработки персональных данных).

ХХХ - трехзначный порядковый номер по Журналу.

2.2.2. МНИ выдаются пользователям ИСПДн с отметкой в Журнале.

2.2.3. Хранение съемных МНИ должно осуществляться в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.2.4. МНИ, после удаления информации, содержащей персональные данные, с учета не снимаются. В дальнейшем эти МНИ могут использоваться для обработки и хранения персональных данных. Если МНИ не пригодны для дальнейшего использования, они подлежат списанию и уничтожению.

2.2.5. О фактах утраты МНИ докладывается ответственному за организацию обработки персональных данных, с внесением записи в Журнал.

2.2.6. Передача МНИ производится ответственным за организацию обработки персональных данных по Журналу.

2.2.7. В случае неисправности МНИ, пользователь сдает его ответственному за организацию обработки персональных данных с внесением в Журнал записи о неисправности МНИ.

2.3. МНИ, утратившие практическое значение или пришедшие в негодность уничтожаются.

3. Порядок уничтожения МНИ

Уничтожение МНИ производится ответственным за организацию обработки персональных данных, путем их физического разрушения, с оформлением акта уничтожения. Перед уничтожением МНИ информация с них должна быть удалена (уничтожена, стерта и т.д.), если это возможно выполнить.

Приложение
к Инструкции по организации учета,
использования и уничтожения
машинных носителей информации,
предназначенных для обработки и
хранения персональных данных

ЖУРНАЛ
учета и выдачи машинных носителей информации, содержащих персональные данные

Начат «____» _____ 201_ г.
Администратор информационной безопасности
_____

№ п/п	Носитель	Учетный номер носителя	Дата передачи носителя	Ф.И.О. получившего	Роспись	Примечание

Приложение № 6
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ИНСТРУКЦИЯ
по правилам обращения с носителями ключевой информации в информационных системах персональных данных

1. Термины и определения

Электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном федеральным законом № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Носитель ключевой информации (далее - ключевой носитель) – машинный носитель информации, содержащий ключ электронной подписи.

2. Общие положения

2.1. Настоящая инструкция предназначена для пользователей информационных систем персональных данных, использующих средства ЭП.

2.2. Инструкция содержит основные правила обращения с ключами ЭП, выполнение которых необходимо для обеспечения защиты информации при

обмене электронными документами.

2.3. Работу с ключами ЭП контролирует администратор безопасности ИСПДн. Администратор безопасности ИСПДн проводит инструктаж с пользователями по правилам изготовления, хранения, обращения и эксплуатации ключей.

2.4. Владелец сертификата ключа проверки ЭП, вырабатывает самостоятельно или в сопровождении администратора безопасности ИСПДн личный ключ ЭП, а также запрос на получение сертификата ключа проверки электронной подписи (в электронном виде и на бумажном носителе).

2.5. Владелец ключа ЭП несет персональную ответственность за безопасность ключей ЭП и обязан обеспечивать их сохранность, неразглашение и нераспространение, несет персональную ответственность за нарушение требований настоящей инструкции.

2.6. Запрещается оставлять без контроля ПЭВМ с незаблокированным сеансом, на котором применяется ЭП.

3. Порядок работы со средствами ЭП

3.1. Учет носителей ключевой информации осуществляет администратор безопасности ИСПДн.

3.2. Ключи ЭП изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В работе используется рабочая копия ключевого носителя.

3.3. При выходе из строя носителя с ключевой информацией пользователь уведомляет об этом администратора безопасности ИСПДн. Администратор безопасности ИСПДн в присутствии пользователя изготовляет копию ключевого носителя с эталонной копии.

3.4. Не позднее, чем за 10 рабочих дней до окончания срока действия ключа ЭП, его владелец обязан выполнить все мероприятия по формированию новых ключей.

3.5. Ключевые носители хранятся в шкафах (сейфах, ящиках, хранилищах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.6. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность неправомерного доступа к ним.

3.7. Ключевые носители должны находиться в пределах контролируемой зоны, за исключением случаев, связанных со служебной необходимостью.

3.8. Не допускается:

осуществлять несанкционированное администратором безопасности ИСПДн копирование ключевых носителей;

передавать носители ключевой информации и (или) их содержимое лицам, не допущенным к ним;

записывать на ключевые носители другую информацию.

4. Действия при компрометации ключей ЭП

4.1. Компрометация ключа ЭП – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

4.2. К событиям, связанным с компрометацией ключей ЭП, относятся, включая, но не ограничивая, следующие:

потеря ключевых носителей;

нарушение правил хранения и уничтожения;

возникновение подозрений на утечку информации или ее искажение;

случаи, когда нельзя установить, что произошло с ключевыми носителями.

4.3. При компрометации ключа ЭП пользователь прекращает обмен электронными документами с другими пользователями и извещает администратора безопасности ИСПДн о факте компрометации.

4.4. По факту компрометации ключей должно быть проведено служебное расследование.

5. Уничтожение ключей ЭП

5.1. Ключи ЭП должны быть выведены из действия и уничтожены в следующих случаях:

плановая смена ключей ЭП;

изменение данных о владельце ЭП;

компрометация ключей;

выход из строя ключевых носителей;

прекращение полномочий владельца ЭП.

5.2. Уничтожение ключей ЭП может производиться путем уничтожения ключевого носителя, на котором они расположены, или путем удаления ключей без повреждения ключевого носителя.

5.3. Ключи ЭП должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

Приложение № 7
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила) в Главном управлении строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края (далее – Главное управление) определяют порядок учета (регистрации) и рассмотрения запросов субъектов персональных данных или их представителей (далее - запросы).

2. Настоящие Правила разработаны в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральным законом от 2 мая 2006 г. N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27 июля 2004 г. N 79-ФЗ «О государственной гражданской службе Российской Федерации», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. N 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.

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

подтверждение факта обработки персональных данных Главным управлением;

правовые основания и цели обработки персональных данных;

цели и применяемые Главным управлением способы обработки персональных данных;

наименование и место нахождения Главного управления, сведения о лицах (за исключением государственных гражданских служащих (работников) Главного управления), которые имеют доступ к персональным

данным или которым могут быть раскрыты персональные данные на основании договора с Главным управлением или на основании федерального закона;

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 законодательством;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные федеральным законодательством.

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

5. Сведения, указанные в пункте 3 настоящих Правил, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

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

обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

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

доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

7. Сведения, указанные в пункте 3 настоящих Правил предоставляются субъекту персональных данных или его представителю Главным управлением при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос 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 Главным управлением (номер служебного контракта (договора), дата заключения служебного контракта (договора), условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Главным управлением, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8. Рассмотрение запросов является служебной обязанностью руководителя, заместителя руководителя и уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.

9. Должностные лица Главного управления обеспечивают:

объективное, всестороннее и своевременное рассмотрения запроса;

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

направление письменных ответов по существу запроса.

10. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

11. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в пункте 3 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Главное управление или направить повторный запрос в целях получения сведений, указанных в пункте 3 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо

выгодоприобретателем или поручителем по которому является субъект персональных данных.

12. Субъект персональных данных вправе обратиться повторно в Главное управление или направить ему повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

13. Главное управление вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 11 и 12 настоящих Правил. Такой отказ должен быть мотивирован.

14. Прошедшие регистрацию запросы в тот же день докладываются начальнику Главного управления либо лицу, ответственному за обработку запросов, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

15. Лицо, ответственное за обработку запросов субъектов персональных данных, при рассмотрении и разрешении запроса обязано:

внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить государственных гражданских служащих (работников) на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

16. Главное управление обязано 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 в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

17. 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 Главного управления обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение пункта 6

настоящих Правил или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

18. Главное управление обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

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, уполномоченные должностные лица Главного управления 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, уполномоченные должностные лица Главного управления обязаны уничтожить такие персональные данные. Главное управление обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

19. 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 уполномоченные должностные лица Главного управления обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. 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 уполномоченные должностные лица Главного управления 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.

20. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица Главного управления 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 или обеспечить их блокирование (если обработка

персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

21. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица Главного управления в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица Главного управления 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 Главное управление обязано уведомить субъекта персональных данных или его представителя, а 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 указанный орган.

22. Ответы на запросы печатаются на бланке Главного управления и регистрируются.

23. Лицо, ответственное за обработку запросов, лично осуществляет контроль за работой с запросами и организацией их приема. На контроль берутся все запросы.

24. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

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

Приложение № 8
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в Главном управлении строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края (далее – Главное управление) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановлением Правительства Российской Федерации от 21 марта 2012 года N 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.

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона.

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Главном управлении проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются ответственным за обеспечение безопасности персональных данных в Главном управлении либо комиссией по обеспечению безопасности информации конфиденциального характера, образованной в Главном управлении.

В проведении проверки не может участвовать государственный гражданский служащий (работник), прямо или косвенно заинтересованный в её результатах.

6. Проверки соответствия обработки персональных данных установленным требованиям в Главном управлении, проводятся на основании приказа начальника Главного управления или на основании поступившего в Главное управление письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

состояние учета машинных носителей персональных данных;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

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

осуществление мероприятий по обеспечению целостности персональных данных.

8. Ответственный за обеспечение безопасности персональных данных в Главном управлении (комиссия по обеспечению безопасности информации конфиденциального характера) имеет право:

запрашивать у государственных гражданских служащих (работников) Главного управления информацию, необходимую для реализации полномочий;

требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить начальнику Главного управления предложения о совершенствовании правового, технического и организационного

регулирования обеспечения безопасности персональных данных при их обработке;

вносить начальнику Главного управления предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. В отношении персональных данных, ставших известными ответственному за обеспечение безопасности персональных данных в комиссии по обеспечению безопасности информации конфиденциального характера в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных. Работа комиссии может носить плановый и внеплановый характер.

10. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, начальнику Главного управления докладывает ответственный за обеспечение безопасности персональных данных либо председатель комиссии по обеспечению безопасности информации конфиденциального характера, в форме письменного заключения.

Приложение № 9
к Положению об обеспечении безопасности персональных данных при их обработке в информационных системах Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

ПРАВИЛА
обработки персональных данных

1. Обработка персональных данных в Главном управлении должна осуществляться на законной и справедливой основе.

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

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

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

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Сотрудник Главного управления, непосредственно осуществляющий обработку персональных данных (далее – Оператор), должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством:

осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 г. № 152-ФЗ (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Главного управления в отношении обработки персональных данных, локальным актам Главного управления;

оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых Главным управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

ознакомление операторов с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Главного управления в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных государственных гражданских служащих (работников).

8. Обеспечение безопасности персональных данных достигается, в частности:

определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

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

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

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

учетом машинных носителей персональных данных;

обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;

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

установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

9. Целями обработки персональных данных государственных гражданских служащих (работников) являются:

обеспечение соблюдения законов и иных нормативных правовых актов;

соблюдение порядка и правил приема на государственную гражданскую службу (прием на работу);

использование в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчётов в вышестоящие органы;

обеспечение личной безопасности сотрудников Главного управления.

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

11. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению Главного управления, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Главного управления. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а 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 указанный орган.

12. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Главного управления) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Главного управления) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Главного управления) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

УТВЕРЖДЕНА
приказом Главного управления
№ 57 от 01.03.2016

ИНСТРУКЦИЯ
ответственного за организацию обработки и обеспечение безопасности персональных данных Главного управления строительства, транспорта, жилищно-коммунального и дорожного хозяйства Алтайского края

1. Общие положения

1.1. Данная инструкция определяет основные функциональные обязанности и права ответственного за организацию обработки и обеспечение безопасности персональных данных.

1.2. Ответственный за организацию обработки и обеспечение безопасности персональных данных непосредственно подчиняется начальнику Главного управления.

2. Обязанности

2.1. Организует проведение внутреннего контроля за соблюдением оператором персональных данных и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

2.2. Организует доведение до сведения работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.3. Организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приемом и обработкой таких обращений и запросов.

3. Полномочия

3.1. Требовать от всех сотрудников, работающих с информационными системами персональных данных (далее - ИСПДн), неукоснительного выполнения нормативных и методических документов по обеспечению защиты информации в ИСПДн. Давать обязательные для исполнения указания по вопросам сохранности информации, содержащей персональные данные.

3.2. Запрашивать информацию и документы, необходимые для выполнения задач, входящих в компетенцию ответственного за организацию обработки персональных данных;

3.3. Организовывать и проводить проверки соблюдения установленных норм и требований информационной безопасности в ИСПДн лицами, допущенными к персональным данным.

4. Ответственность

4.1. Ответственный за организацию обработки и обеспечение безопасности персональных данных несет дисциплинарную, административную и иную ответственность в соответствии с действующим законодательством Российской Федерации.