КОМИТЕТ
ПО ДЕЛАМ ЗАПИСИ АКТОВ
ГРАЖДАНСКОГО СОСТОЯНИЯ И АРХИВОВ
РЕСПУБЛИКИ АЛТАЙ

(КОМИТЕТ ПО ДЕЛАМ ЗАГС И АРХИВОВ
РЕСПУБЛИКИ АЛТАЙ)

АЛТАЙ РЕСПУБЛИКАНЫҢ
ГРАЖДАН АЙАЛГАНЫ БИЧИИР ЛЕ
АРХИВТЕР КЕРЕКТЕРИ ААЙЫНЧА
КОМИТЕДИ

(АЛТАЙ РЕСПУБЛИКАНЫҢ ЗАГС-ТЫҢ
ЛЕ АРХИВТЕР КОМИТЕДИ)

ПРИКАЗ

23.12.2020 94/1

г. Горно-Алтайск

Об утверждении перечня документов, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ«О персональных данных»

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных », Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», реализуя Постановление 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. Утвердить:

1.1. Правила обработки персональных данных в Комитете по делам ЗАГС и архивов Республики Алтай (далее – Комитет), устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие 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 (приложение № 1);

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей (приложение № 2);

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных в Комитете требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора (приложение № 3);

1.4. Правила работы в Комитете с обезличенными данными (приложение № 4);

1.5. Перечни персональных данных, обрабатываемых в Комитете в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций (приложение № 5);

1.6. Перечень должностей служащих Комитета, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (приложение № 6);

1.7 Перечень должностей Комитета, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение № 7);

1.8. Должностную инструкцию лица, ответственного за организацию обработки персональных данных в Комитете (приложение № 8);

1.9. Типовое обязательство государственного служащего Комитета, непосредственно осуществляющего обработку персональных данных, о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае расторжения с ним служебного контракта (приложение № 9);

1.10. Типовое обязательство работника Комитета, непосредственно осуществляющего обработку персональных данных, о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае расторжения с ним трудового договора (приложение № 10)

1.11. Типовая форма согласия на обработку персональных данных государственного служащего Комитета (приложение № 11);

1.12. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи с поступлением на работу, ее выполнением в Комитете (приложение № 12);

1.13. Порядок доступа работников Комитета в помещения, в которых ведется обработка персональных данных. (приложение № 13)

1.14. Политика обработки персональных данных, обрабатываемых в Комитете. (приложение № 14)

1.15. План проведения внутреннего контроля обработки персональных данных Комитета. (приложение № 15)

1.16. Форму акта контроля соответствия обработки персональных данных. (приложение № 16)

1.17. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Комитете. (Приложение № 17)

1.18. Акт оценки вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых оператором мер. (приложение № 18)

1.19. Инструкцию по организации парольной защиты в Комитете. (приложение № 19)

1.20 Инструкцию по применению средств антивирусной защиты в Комитете. (приложение № 20)

1.21. Регламент по установке и использованию разрешённого программного обеспечения в Комитете. (приложение № 21)

1.22. Перечень разрешённого программного обеспечения в Комитете. (приложение № 22)

1.23. Матрицу доступа к персональным данным в Комитете. (приложение № 23)

1.24. Перечень мест хранения персональных данных на бумажных носителях в Комитете. (приложение № 24)

1.25. Журнал учёта обращений или запросов субъектов персональных данных в Комитете. (приложение № 25)

2. Довести настоящее распоряжение до сведения всех государственных служащих и работников Комитета.

3. Признать утратившим силу приказ от 15.12.2015 № 99 «Об утверждении перечня документов, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»

4. Настоящий приказ подлежит опубликованию на официальном сайте Комитета.

Председатель Антарадонова Н.П.

Ознакомлен 23.12.2020

Приложение №1
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие 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. Обработка персональных данных должна осуществляться на законной 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. 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:

1) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006г. №152-ФЗ (далее - Федеральный закон);

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

3) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8. Обеспечение безопасности персональных данных достигается, в частности:

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

2) 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;

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

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

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

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

8) 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 работников являются:

1) обеспечение соблюдения законов и иных нормативных правовых актов;

2) учет работников в учреждении;

3) соблюдение порядка и правил приема в учреждение;

4) 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;

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

6) обеспечение личной безопасности работников.

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 оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан 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, 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 оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) 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 Федеральным законом.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3-х дней с даты получения указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных

данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

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 оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

Приложение №2
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Правила
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение сведений, указанных в пункте 7 настоящих Правил, за исключением случаев, предусмотренных пунктом 6 настоящих Правил. Субъект персональных данных вправе требовать от оператора 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.

2. Сведения, указанные в пункте 7 настоящих Правил, должны быть предоставлены субъекту персональных данных оператором 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.

3. Сведения, указанные в пункте 7 настоящих Правил, предоставляются субъекту персональных данных или его представителю оператором 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 оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, 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.

4. В случае, если сведения, указанные в пункте 7 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте настоящих правил, и ознакомления с такими персональными данными не ранее чем через 30 (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.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 7 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 4 настоящих Правил, 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 наряду со сведениями, указанными в пункте 3 настоящих Правил, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 4 и 5 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

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

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – федеральный закон);

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

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

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

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

9) иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

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

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

2) 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;

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

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

5) 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.

9. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

1) Оператор обязан сообщить в порядке, предусмотренном пунктами 1-8 настоящих Правил, 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 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

2) 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 оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на пункт 8

настоящих Правил, в соответствии с федеральным законом, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

10. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (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, оператор обязан уничтожить такие персональные данные. Оператор обязан 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.

11. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Приложение №3
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Правила
осуществления 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 оператора

Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Комитете определяются 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.

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Комитете организовывается проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных.

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

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

осуществление мероприятий по обеспечению целостности персональных данных.

Должностное лицо, ответственное за организацию обработки персональных данных в Комитете имеет право:

запрашивать у сотрудников Комитета 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 председателю Комитета предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

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

В отношении персональных данных, ставших известными должностному лицу, ответственному за организацию обработки персональных данных в Комитете в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, председателю Комитета докладывает ответственный за организацию обработки персональных данных в форме письменного заключения.

Председатель Комитета, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

Приложение №4
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Правила
работы с обезличенными данными

1. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4. Для обезличивания персональных данных годятся любые способы, явно не запрещенные законодательно.

5. Председатель Комитета принимает решение о необходимости обезличивания персональных данных.

6. Должностное лицо, ответственное за организацию обработки персональных данных готовит предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

7. Сотрудники подразделений, обслуживающие базы с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

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

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

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

10.1. парольной политики;
10.2. антивирусной политики;
10.3. правил работы со съемными носителями (если они используются);
10.4. правил резервного копирования;
10.5. правил доступа в помещения, где расположены элементы информационных систем;
11. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
11.1. правил хранения бумажных носителей;
11.2. правил доступа к ним и в помещения, где они хранятся.

Приложение №5
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Перечни
персональных данных, обрабатываемых в Комитете,
в связи с реализацией трудовых отношений, а также в связи
с оказанием государственных услуг и осуществлением государственных функций

Комитет обрабатывает следующие категории персональных данных.

В связи с реализацией служебных (трудовых) отношений:

1. Фамилия, имя, отчество.
2. Дата рождения (число, месяц, год).
3. Место рождения.
4. Гражданство.
5. Образование, квалификация, послевузовское профессиональное образование.
6. Классный чин, дипломатический ранг, воинское или специальное звание.
7. Судимость.
8. Допуск к государственной тайне.
9. Трудовая деятельность.
10. Государственные награды.
11. Семейное положение, в том числе сведения о супруге, бывшем супруге, близких родственниках.
12. Адрес (место жительства), место регистрации.
13. Воинская обязанность.
14. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера.
15. Наличие (отсутствие) заболеваний.
16. СНИЛС.
17. ИНН.
18. Документ, удостоверяющий личность.
19. Пол (мужской/женский).
20. Биометрические: фотография (личное дело сотрудника).

В связи с оказанием государственных услуг и осуществлением государственных функций:

1. Фамилия, имя, отчество.
2. Дата рождения (число, месяц, год).
3. Место рождения.
4. Гражданство.
5. Адрес (место жительства), место регистрации.
6. Семейное положение.
7. Образование, квалификация.
8. Национальность.
9. Документ, удостоверяющий личность.
10. Пол (мужской/женский).
11. Дата смерти (число, месяц, год).
12. Место смерти.
13. Причина смерти.
14. Серия медицинского свидетельства о рождении.
15. Номер медицинского свидетельства о рождении.
16. Серия медицинского свидетельства о смерти.
17. Номер медицинского свидетельства о смерти.
14. Дата записи акта гражданского состояния.
15. Номер записи акта гражданского состояния.
16. Серия свидетельства о государственной регистрации акта гражданского состояния.
17. Номер свидетельства о государственной регистрации акта гражданского состояния.

Приложение №6
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Перечень
должностей служащих Комитета,
ответственных за проведение мероприятий
по обезличиванию обрабатываемых персональных данных

1. Ответственные за проведение мероприятий по обезличиванию обрабатываемых в Комитете персональных данных:
- Панов Роман Владимирович – системный администратор Комитета по делам ЗАГС и архивов Республики Алтай.

Приложение №7
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Перечень должностей Комитета, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Председатель Комитета
2. Главный бухгалтер
3. Бухгалтер
4. Специалист – эксперт
5. Специалист по кадрам
6. Документовед
7. Системный администратор
8. Начальник отдела ЗАГС.
9. Начальник отдела по делам архивов
10. Главный специалист 1 разряда
11. Главный специалист 2 разряда
12. Главный специалист 3 разряда

Приложение №8
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Должностная инструкция
лица, ответственного за организацию
обработки персональных данных в Комитете

1. Должностное лицо, ответственное за организацию обработки персональных данных должно руководствоваться в своей деятельности Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», нормативными правовыми актами Комитета в области защиты персональных данных, настоящей должностной инструкцией.

2. Должностное лицо, ответственное за организацию обработки персональных данных обязано:

- осуществлять внутренний контроль за соблюдением работниками Комитета требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доводить до сведения работников Комитета положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- осуществлять контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей;

- предоставлять субъекту персональных данных по его просьбе информацию;

- разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

Приложение №9
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Типовое обязательство
государственного служащего Комитета,
непосредственно осуществляющего обработку персональных данных,
о прекращении обработки персональных данных, ставших известными
ему в связи с исполнением должностных обязанностей,
в случае расторжения с ним служебного контракта

Председателю Комитета
По делам ЗАГС и архивов Республики Алтай
_____
от_____
(ФИО, должность)

Заявление.

Я,_____,
проживающий (ая) по адресу:_____
паспорт серия _____ №_____, выданный (кем и когда)
_____
_____предупрежден (а) о том, что на период исполнения мною должностных обязанностей по служебному контракту о прохождении государственной гражданской службы Республики Алтай и замещении должности государственной гражданской службы Республики Алтай, заключенному между мною и Комитетом по делам ЗАГС и архивов Республики Алтай (далее – Комитет), и предусматривающих работу с персональными данными мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

- не передавать (в любом виде) и не разглашать третьим лицам и работникам Комитета, не имеющим на это право в силу выполняемых ими должностных обязанностей, информацию, содержащую персональные данные сотрудников (граждан), которая мне доверена или станет известной в связи с исполнением должностных обязанностей;

- в случае попытки третьих лиц или сотрудников Комитета, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или вышестоящему руководителю;

- не использовать информацию, содержащую персональные данные с

целью получения выгоды;

- выполнять требования закона и иных нормативных правовых актов Российской Федерации, а так же внутренних документов Комитета, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

- после прекращения моих прав на допуск к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным или прекращения служебного контракта), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Комитета, известную мне информацию, содержащую персональные данные.

- в случае расторжения со мной служебного контракта прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

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

«___» _____ 20__ года _____ _____
(подпись) (ФИО)

Приложение №10
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Типовое обязательство
работника Комитета, непосредственно осуществляющего обработку персональных данных, о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае расторжения с ним трудового договора

Председателю Комитета
По делам ЗАГС и архивов Республики Алтай

_____

от_____

(ФИО, должность)

Заявление.

Я,_____,
проживающий (ая) по адресу:_____
паспорт серия _____ №_____, выданный (кем и когда)
_____
_____предупрежден (а) о том, что на период исполнения мною должностных обязанностей по трудовому договору, заключенному между мною и Комитетом по делам ЗАГС и архивов Республики Алтай (далее – Комитет), и предусматривающих работу с персональными данными мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

- не передавать (в любом виде) и не разглашать третьим лицам и работникам Комитета, не имеющим на это право в силу выполняемых ими должностных обязанностей, информацию, содержащую персональные данные сотрудников (граждан), которая мне доверена или станет известной в связи с исполнением должностных обязанностей;

- в случае попытки третьих лиц или сотрудников Комитета, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или вышестоящему руководителю;

- не использовать информацию, содержащую персональные данные с целью получения выгоды;

- выполнять требования закона и иных нормативных правовых актов Российской Федерации, а так же внутренних документов Комитета, регламентирующих вопросы защиты интересов субъектов персональных

данных, порядка обработки и защиты персональных данных;

- после прекращения моих прав на допуск к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным или расторжения трудового договора), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Комитета, известную мне информацию, содержащую персональные данные.

- в случае расторжения со мной трудового договора прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

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

«___» _____ 20__ года _____ _____
(подпись) (ФИО)

Приложение №11
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Председателю Комитета

По делам ЗАГС и архивов Республики Алтай

_____

от_____

(ФИО, должность)

Типовая форма согласия
на обработку персональных данных
государственного служащего, работников Комитета

Я,_____,
проживающий (ая) по адресу:_____
паспорт серия _____ №_____, выданный (кем и когда)
_____
в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,
в целях:_____
(указать цели обработки персональных данных)

даю свое согласие на обработку своих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, совершаемые с использованием средств автоматизации или без использования таких средств.

Подтверждаю, что ознакомлен(а) с Положением о работе с персональными данными, утвержденными приказом Комитета по делам ЗАГС и архивов № от, права и обязанности в области защиты персональных данных мне разъяснены.

Настоящее согласие действует до истечения определяемых в соответствии с федеральным законодательством и законодательством Республики Алтай области сроков хранения персональных данных.

Оставляю за собой право отзыва данного согласия по моему письменному заявлению. Всю ответственность за неблагоприятные последствия отзыва согласия беру на себя.

_____ / _____ /
(подпись) (дата)
Принял _____ _____
(подпись) (дата)

Приложение №12
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

Я,_____
_____,
проживающий (ая) по адресу:_____
паспорт серия _____ №_____, выданный (кем и когда)
_____
в соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» настоящим подтверждаю, что мне разъяснены юридические последствия отказа предоставить свои персональные данные.

«____»_____ _____
дата подпись

Приложение №13
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Порядок
доступа работников Комитета в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа государственных служащих и работников Комитета (далее – Работники) в помещения, в которых ведется обработка персональных данных, (далее – Порядок) устанавливают единые требования к доступу Работников Комитета в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Комитете, и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми Работниками Комитета.

3. Помещения, в которых ведется обработка персональных данных, должны отвечать определенным нормам и исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации.

4. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

5. По завершению рабочего дня, помещения, в которых ведется обработка персональных данных, закрываются.

6. Вскрытие помещений, где ведется обработка персональных данных, производят Работники, работающие в этих помещениях.

7. При отсутствии сотрудников Комитета, работающих в этих помещениях, помещения могут быть вскрыты комиссией, созданной по указанию председателя Комитета.

8. В случае утраты ключей от помещений немедленно заменяется замок.

9. Уборка в помещениях, где ведется обработка персональных данных, производится только в присутствии служащих, работающих в этих помещениях.

10. При обнаружении повреждений запоров или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка персональных данных, посторонних лиц, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность председатель Комитета и органы МВД.

11. Одновременно принимаются меры по охране места происшествия и до прибытия работников органов МВД в эти помещения никто не допускается.

Приложение №14
к приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
от 23.12.2020 № 94/1

Политика обработки персональных данных Комитета по делам ЗАГС и архивов Республики Алтай

1. Общие положения.

1.1. Политика обработки персональных данных в Комитете по делам ЗАГС и архивов Республики (далее — Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в Комитете по делам ЗАГС и архивов Республики Алтай (далее - Комитет) персональных данных, функции Комитета при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Комитете требования к защите персональных данных.

1.2. Политика разработана с учетом требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

1.3. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в Комитете вопросы обработки персональных данных работников Комитета и других субъектов персональных данных.

2. Законодательные и иные нормативные правовые акты Российской Федерации, в соответствии с которыми определяется Политика обработки персональных данных в Комитете

2.1. Политика обработки персональных данных в Комитете определяется в соответствии со следующими нормативными правовыми актами:

Конституция Российской Федерации;

Трудовой кодекс Российской Федерации;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

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

постановление Правительства Российской Федерации от 6 июля 2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

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

приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

2.2. В целях реализации положений Политики в Комитете разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

положение об обработке персональных данных;

положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных;

перечень должностей структурных подразделений Комитета, при замещении которых осуществляется обработка персональных данных;

иные локальные нормативные акты и документы, регламентирующие в Комитете вопросы обработки персональных данных.

3. Основные термины и определения, используемые в локальных нормативных актах Комитета, регламентирующих вопросы обработки персональных данных

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

Информация — сведения (сообщения, данные) независимо от формы их представления.

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.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемые 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.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

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

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

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

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

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.

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

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4. Принципы и цели обработки персональных данных

4.1. Комитет, являясь оператором персональных данных, осуществляет обработку персональных данных работников Комитета и других субъектов персональных данных, не состоящих с Комитетом в трудовых отношениях.

4.2. Обработка персональных данных в Комитете осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Комитета и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

обработка персональных данных осуществляется в Комитете на законной и справедливой основе;

обработка персональных данных ограничивается достижением конкретных, заранее определенных 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. •Комитетом 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.

4.3. Персональные данные обрабатываются в Комитете в целях:
обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Комитета;

осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Комитет, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

регулирования трудовых отношений с работниками Комитета; защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

подготовки, заключения, исполнения и прекращения договоров с контрагентами;

обеспечения пропускного и внутриобъектового режимов на объектах Комитета;

формирования справочных материалов для внутреннего информационного обеспечения деятельности Комитета ;

исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

осуществления прав и законных интересов Комитета в рамках осуществления установленных видов деятельности, или третьих лиц либо достижения общественно значимых целей; в иных законных целях.

5. Перечень субъектов, персональные данные которых обрабатываются в Комитете

5.1. В Комитете обрабатываются персональные данные следующих категорий субъектов:

- работники структурных подразделений Комитета;
- другие субъекты персональных данных (для обеспечения реализации целей обработки, указанных в разделе 4 Политики).

6. Перечень персональных данных, обрабатываемых в Комитете

6.1 Перечень персональных данных, обрабатываемых в Комитете, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Комитета с учетом целей обработки персональных данных, указанных в разделе 4 Политики.

6.2. Осуществляется обработка специальной категории персональных данных - национальность.

7. Функции Комитета при осуществлении обработки персональных данных

7.1. Комитет при осуществлении обработки персональных данных:

принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Комитета в области персональных данных;

принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

назначает лицо, ответственное за организацию обработки персональных данных в Комитете;

издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Комитете;

осуществляет ознакомление работников Комитета, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Комитета в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных работников;

публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

8. Условия обработки персональных данных в Комитете

8.1. Обработка персональных данных в Комитете осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

8.2. Комитет без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральными законами.

8.3. Комитет вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

8.4. В целях внутреннего информационного обеспечения Комитет может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения,

адрес, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

8.5. Доступ к обрабатываемым в Комитете персональным данным разрешается только работникам Комитета, занимающим должности, включенные в перечень должностей структурных подразделений Комитета, при замещении которых осуществляется обработка персональных данных.

9. Перечень действий с персональными данными и способы их обработки

9.1. Комитет осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

9.2. Обработка персональных данных в Комитета осуществляется следующими способами:

неавтоматизированная обработка персональных данных; автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

смешанная обработка персональных данных.

10. Права субъектов персональных данных

10.1. Субъекты персональных данных имеют право на: полную информацию об их персональных данных, обрабатываемых в Комитете;

доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом, а также на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

отзыв согласия на обработку персональных данных; принятие предусмотренных законом мер по защите своих прав; обжалование действия или бездействия Комитета, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в

уполномоченный орган по защите прав субъектов персональных данных или в суд;

осуществление иных прав, предусмотренных законодательством Российской Федерации.

11. Меры, принимаемые Комитете для обеспечения выполнения обязанностей оператора при обработке персональных данных

11.1. Меры, необходимые и достаточные для обеспечения выполнения Комитетом обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

назначение лица, ответственного за организацию обработки персональных данных в Комитете;

принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;

организацию обучения и проведение методической работы с работниками структурных подразделений Комитета, занимающими должности, включенные в перечень должностей структурных подразделений Комитета, при замещении которых осуществляется обработка персональных данных;

получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;

обеспечение раздельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;

установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны, сети «Интернет» без применения установленных в Комитете мер по обеспечению безопасности персональных данных (за исключением общедоступных и (или) обезличенных персональных данных);

хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;

осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Комитета;

иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

11.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами Комитета, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Комитета.

12. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Комитета в области персональных данных, в том числе требований к защите персональных данных

12.1. Контроль за соблюдением структурными подразделениями Комитета законодательства Российской Федерации и локальных нормативных актов Комитета в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в структурных подразделениях Комитета законодательству Российской Федерации и локальным нормативным актам Комитета в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

12.2. Внутренний контроль за соблюдением структурными подразделениями Комитета законодательства Российской Федерации и локальных нормативных актов Комитета в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в Комитете.

12.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Комитета осуществляет Председатель Комитета.

12.4. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов Комитета в области персональных данных, а также за обеспечение конфиденциальности и безопасности персональных данных возлагается на Председателя Комитета.

Приложение №15
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

План проведения
внутреннего контроля обработки персональных данных
Комитете по делам ЗАГС и архивов Республики Алтай

№ п/п	Мероприятие	Срок проведения
1	Проверка полноты, качества и актуальности внутренних распорядительных документов, регламентирующих обработку и обеспечение безопасности персональных данных	Ежегодно
2	Контроль выполнения требований по режиму доступа в помещение, где ведется обработка персональных данных	Ежегодно
3	Проверка порядка использования технических средств защиты	Ежегодно
4	Соблюдение порядка уточнения, блокирования и уничтожения персональных данных	Ежегодно
5	Работа с обращениями субъектов персональных данных	Ежегодно
6	Проверка актуальности сведений в Реестр операторов персональных данных Роскомнадзора	Ежегодно
7	Подведение итогов	Ежегодно
8	Устранение недостатков	Ежегодно
9	Составление акта внутреннего контроля	Ежегодно
10	Доклад председателю Комитета	Ежегодно

Приложение №16
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

АКТ
контроля соответствия обработки персональных данных в Комитете по делам ЗАГС и архивов Республики Алтай

В соответствии с п.4 ч.1 ст. 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ « О персональных данных» в Комитете по делам ЗАГС и архивов Республики Алтай проведен контроль соответствия обработки персональных данных следующим актам:

- Федеральному закону от 27.07.2006 г. №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативно правовым актам, требованиям к защите персональных данных, в том числе «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением Правительства от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и «Требованиям к защите персональных данных при их обработки в информационных системах персональных данных», утвержденных постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Иным локальным актам.

В результате проведения внутреннего контроля выявлены нарушения:

_____
_____
_____

Меры по устранению нарушений:

_____
_____Сро

к устранения нарушений:

_____
_____
_____

Ответственный _____ _____\
«____» _____20___г.

Приложение №17
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

ПРАВИЛА
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Комитете по делам ЗАГС и архивов Республики Алтай

1. Общие положения

1.1. Настоящие Правила оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению в Комитет по делам ЗАГС и архивов Республики Алтай (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон N 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом N 152-ФЗ.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2. Основные понятия

2.1. В настоящих Правилах используются основные понятия:

Информация - сведения (сообщения, данные) независимо от формы их представления.

Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

Оценка возможного вреда - определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. Методика оценки возможного вреда субъектам персональных данных

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 безопасности информации:

- неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;
- неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
- неправомерное изменение персональных данных является нарушением целостности персональных данных;
- нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;
- нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
- 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;
- неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
- принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом

затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

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

- убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

- морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4. В оценке возможного вреда Комитет по делам ЗАГС и архивов Республики Алтай исходит из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:

- низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных либо только нарушение доступности персональных данных;

- средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

- высокий уровень возможного вреда - во всех остальных случаях.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых оператором мер

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, назначенным соответствующим приказом, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении, после чего согласовывается с ответственным в Комитет по делам ЗАГС и архивов Республики Алтай за организацию обработки персональных данных и утверждается Председателем Комитета по делам ЗАГС и архивов Республики Алтай.

4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом N 152-ФЗ,

определяется лицом, ответственным в Комитет по делам ЗАГС и архивов Республики Алтай за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение №18
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Акт
оценки вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых оператором мер

N п\п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1.	1. 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	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечением безопасности персональных данных
		Целостность			
		Доступность			
		Конфиденциальность	+		
2.	2. Порядок и условия применения средств защиты информации	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты информационной системы персональных данных
		Целостность	+		
		Доступность			
		Конфиденциальность			
3.	3. Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных	Убытки и моральный вред	+	высокий	Программа и методика испытаний систем защиты
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		

4.	4. Состояние учета машинных носителей персональных данных	Убытки и моральный вред	+	высокий	Инструкция по учету машинных носителей информации
		Целостность			
		Доступность			
		Конфиденциальность	+		
5	5. Соблюдение правил доступа к персональным данным	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
		Целостность	+		
		Доступность			
		Конфиденциальность	+		
6	6. Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер	Убытки и моральный вред	+	высокий	Мониторинг средств защиты информации на наличие фактов доступа к персональным данным
		Целостность			
		Доступность			
		Конфиденциальность	+		
7	7. Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки и моральный вред		средний	Применение резервного копирования
		Целостность	+		
		Доступность	+		
		Конфиденциальность			
8	8. Осуществление мероприятий по обеспечению целостности персональных данных	Убытки и моральный вред		низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность			
		Конфиденциальность			

Приложение №19
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Инструкция по организации парольной защиты в Комитете по делам ЗАГС и архивов Республики Алтай

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в Комитете по делам ЗАГС и архивов Республики Алтай.

1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за соблюдение норм антивирусной защиты учреждения. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати

владельцев паролей (при их наличии у исполнителей), либо печать учреждения.

3. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в квартал.

4. Внеплановая смена личного пароля или удаление учетной записи пользователя ПК в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться уполномоченными сотрудниками – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ПК организации.

6. В случае компрометации личного пароля пользователя ПК должны быть немедленно предприняты меры в соответствии с п.4 или п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за соблюдение норм парольной защиты или руководителя учреждения в опечатанном личной печатью пенале.

8. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за соблюдение норм парольной защиты.

Приложение №20
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты на средствах вычислительной техники (далее - СВТ) Комитета по делам ЗАГС и архивов Республики Алтай (далее - Комитет), а также устанавливает ответственность за их выполнение.

Настоящая инструкция обязательна для выполнения всеми сотрудниками Комитета.

Инструкция по применению средств антивирусной защиты

1.1 Защита программного обеспечения СВТ от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

1.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами ФСТЭК и ФСБ России.

1.3 Решение задач по установке и сопровождению средств антивирусной защиты возлагается на администратора информационной безопасности Комитета.

1.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

1.5 Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты.

1.6 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.

1.7 Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места администратора информационной безопасности.

1.8 Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах Комитета.

1.9 Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.

1.10 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы) хранящаяся на АРМ, получаемая и

передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

1.11 Процедура обновления баз средства антивирусной защиты должна проводиться не реже одного раза в день на всех СВТ, работающих в сети, не реже 1 (Одного) раза в неделю для всех СВТ, работающих автономно;

1.12 Контроль входящей информации необходимо проводить непосредственно после ее приема.

1.13 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

1.14 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором информационной безопасности Комитета на предмет отсутствия вредоносного программного обеспечения;

1.15 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

1.16 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль СВТ либо обратиться к администратору информационной безопасности Комитета.

1.17 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса администратору информационной безопасности Комитета;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к администратору информационной безопасности Комитета;

1.18 По факту обнаружения зараженных вирусом файлов администратору информационной безопасности Комитета должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

1.19 Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на СВТ.

1.20 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных

антивирусных средств.

1.21 Администратор информационной безопасности Комитета должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

Приложение №21
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Регламент по установке и использованию разрешённого программного обеспечения

1. Общие положения

1.1 Настоящий регламент определяет порядок организации работ по установке и использованию программного обеспечения в Комитете по делам ЗАГС и архивов Республики Алтай (далее - Комитет).

1.2 Настоящий регламент обязателен для исполнения всеми лицами, использующими программное обеспечение Комитета.

2. Термины и определения

2.1 Программное обеспечение (далее - ПО) - компьютерные программы, полученные Комитетом, а также распространяемые на основании свободной лицензии, применяемые для решения задач административно-хозяйственной, финансовой деятельности, а такжеустановленные и используемые на компьютерах, принадлежащих Комитету.

2.2 Пользователь ПО – сотрудники Комитета, на законных основаниях использующие в работе принадлежащие Комитету компьютеры и установленное на них ПО.

2.3 Специалист, обслуживающий ПО – системный администратор Комитета, который имеет допуск к операциям с ПО.

3. Права и обязанности пользователя программного обеспечения

3.1 Пользователь допускается к использованию в работе компьютеров и установленного на них ПО в порядке и объеме, не противоречащем законодательству Российской Федерации и локальным актам Комитета.

3.2 Пользователю запрещается:

- устанавливать самостоятельно ПО;

- вносить изменения в установленное ПО (включая обновление версии продукта);
- удалять ПО.

4. Права и обязанности системного администратора

4.1 Системный администратор принимает решение:
- об установке приобретенного Комитетом ПО в соответствии с условиями соответствующей лицензии;
- о внесении изменений в установленное ПО, включая обновление версии программного продукта;
- об удалении неиспользуемого или поврежденного ПО, а также ПО, использование которого может причинить вред имуществу Комитета;
- о проведении работ по восстановлению ПО из резервных копий в соответствии с документацией на используемое ПО;
- об установке или удалении свободно распространяемого ПО.

4.2 Системный администратор обеспечивает:
- установку ПО;
- внесение изменений в установленное ПО (включая обновление версии продукта);
- удаление ПО;
- настройку установленного ПО;
- контроль исполнения требований лицензионных соглашений установленного ПО;
- поддержку ПО в работоспособном состоянии;
- мониторинг установленного ПО;
- резервное копирование баз данных, подключенных к ПО;
- проведение работ по восстановлению ПО из резервных копий в соответствии с документацией на используемое ПО;
- информирование Председателя Комитета о выявленных нарушениях;
- ведение перечня разрешённого программного обеспечения и его актуализации раз в полгода (приложение №22).

5. Порядок установки и обновлений ПО

5.1 Установка ПО производится с дистрибутивов, полученных с официальных источников.

5.2 Перед установкой обязательно проверяется контрольная сумма дистрибутива на соответствие с эталоном, а также антивирусная проверка. Различие в контрольных суммах полученного дистрибутива и эталона свидетельствует о модификации первого и дальнейшая установка строго запрещена.

5.3 Установка, обновление, удаление средств защиты информации (СЗИ) и средств криптографической информации (СКЗИ) производится в соответствии с формулярами на эти продукты.

5.4 Системный администратор регулярно проверяет наличие обновлений ПО, обязательна установка обновлений безопасности в кратчайшие сроки, которыми разработчик закрывает уязвимости ПО. Для выявления уязвимостей в используемом ПО используется банк данных угроз безопасности информации ФСТЭК, размещённый на ресурсе https://bdu.fstec.ru/.

5.5 В случае, если установленное ПО имеет подключение к базе данных, перед обновлением необходимо сделать резервную копию базы данных.

7. Ответственность

7.1 Пользователь, нарушивший пункт 3.2 настоящего регламента, несет ответственность, установленную действующим законодательством Российской Федерации и локальными актами Комитета.

7.2 Системный администратор несет ответственность за ненадлежащее исполнение или неисполнение обязанностей, предусмотренных пунктами 4.1, 4.2 и 5.1 настоящего регламента, в соответствии с действующим законодательством Российской Федерации.

Приложение №22
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Перечень разрешённого программного обеспечения в Комитете по делам ЗАГС и архивов Республики Алтай

№ П/П	Наименование программного обеспечения	Назначение
1	Microsoft Windows 7 Professional	Операционная система
2	Microsoft Windows 10 Pro	Операционная система
3	Microsoft Windows Server 2012 R2	Операционная система
4	Astra Linux Special Edition (Воронеж)	Операционная система
5	РЭД ОС	Операционная система
6	Microsoft Office 2007	Офисный пакет
7	Microsoft Office 2012	Офисный пакет
8	Microsoft Office 2016	Офисный пакет
9	Р7-Офис	Офисный пакет
10	Мой Офис	Офисный пакет
11	Libre Office	Офисный пакет
12	7-zip	Архиватор
13	Google Chrome	Браузер
14	Microsoft Edge	Браузер
15	Яндекс.Браузер	Браузер
16	Mozilla Firefox	Браузер
17	Kaspersky Endpoint Security 11	Антивирусное ПО

18	Kaspersky Security 11 для Windows Server	Антивирусное ПО
19	Kaspersky Security Center	Администрирование антивирусного ПО
20	Dr.Web	Антивирусное ПО
22	СЭД "Дело" (клиентская часть)	Система электронного документооборота
23	СЭД "Дело" (серверная часть)	Система электронного документооборота
24	Foxit Phantom	Просмотр PDF-файлов
25	ABBYY Fine Reader 10 Professional	Рекдактор PDF-файлов, распознавание текста
26	клиент для подключения к ГИС АФХД	Специализированное ПО
27	клиент для предоставления отчетности "СВОД-СМАРТ"	Специализированное ПО
28	клиент для предоставления отчетности "СБИС"	Специализированное ПО
29	СБИС Плагин	Специализированное ПО
30	КриптоПро CSP 4.0	криптографический провайдер
31	КриптоПро CSP 5.0	криптографический провайдер
32	ViPNet CSP	криптографический провайдер
33	КриптоАРМ ГОСТ	ПО для создания и проверки электронной подписи
34	ViPNet Client 4	ПО для создания защищенных каналов связи при помощи шифрования
35	ViPNet Client 4U for Linux	ПО для создания защищенных каналов связи при помощи шифрования
36	Континент TLS	ПО для создания защищенных каналов связи при помощи шифрования
37	АИС "Госзаказ"	Специализированное ПО
38	СПО "Справки БК"	Специализированное ПО
39	КриптоПро ЭЦП Browser plug-in	Специализированное ПО
40	Плагин для работы с порталом государственных услуг	Специализированное ПО

Приложение №23
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Должность/Объект доступа	АРМ пользователя	СБИС	ГИС АФХД Бухгалтерия	ГИС АФХД Кадры	ФГИС Управления кадровым составом	ФГИС "ЕГР ЗАГС"	ССТУ.РФ	Личные дела сотрудников на бумажных носителях	Заявления граждан, записи актов на бумажных носителях (ЗАГС)	архивные документы на бумажных носителях, содержащие ПДН	ФГИС "ЕРП"	ТОР КНД
Председатель	R,W,CR,D	R,W,CR,D	R	R	R	R	R,W,CR,D	R	R	R	R,W,CR,D	R,W,CR,D
Главный бухгалтер	R,W,CR,D	R,W,CR,D	R,W,CR,D	X	X	X	X	X	X	X	X	X
Бухгалтер	R,W,CR,D	R,W,CR,D	R,W,CR,D	X	X	X	X	X	X	X	X	X
Специалист-эксперт	R,W,CR,D	X	X	X	X	X	R	X	X	X	X	X
Специалист по кадрам	R,W,CR,D	R,W,CR,D	X	R,W,CR,D	R,W,CR,D	X	X	R,W,CR	X	X	X	X
Документовед (комитет)	R,W,CR,D	X	X	X	X	X	R,W,CR,D	X	X	X	X	X
Документовед (ЗАГС)	R,W,CR,D	X	X	X	X	R,W,CR	X	X	R,W,CR	X	X	X
Начальник отдела по делам архивов	R,W,CR,D	X	X	X	X	X	X	X	X	R,W,CR	X	X
Главный специалист 1 разряда	R,W,CR,D	X	X	X	X	R,W,CR	X	X	R,W,CR	X	X	X
Главный специалист 2 разряда	R,W,CR,D	X	X	X	X	R,W,CR	X	X	R,W,CR	X	X	X
Главный специалист 2 разряда отдела по делам архивов	R,W,CR,D	X	X	X	X	X	X	X	X	R,W,CR	R,W,CR,D	R,W,CR,D
Главный специалист 3 разряда	R,W,CR,D	X	X	X	X	R,W,CR	X	X	R,W,CR	X	X	X
Начальник отдела ЗАГС	R,W,CR,D	X	X	X	X	R,W,CR,D	X	X	R,W,CR	X	X	X
Системный администратор	R,W,CR,D, S,U,C,UPD	X	X	X	X	R	R,W,CR,D	X	X	X	X	X

R - чтение документа/файла/каталога
W - изменение/запись документа/файла/каталога
D - удаление документа/файла/каталога
CR - создание документа/файла/каталога
S - установка программ
U - удаление программ
C - настройка программ
UPD - обновление программ
X - нет доступа

Приложение №24
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Перечень
мест хранения материальных носителей персональных данных и ответственных лиц Комитета по делам ЗАГС и архивов Республики Алтай

№ п/п	Адрес, номер или название помещения	Место хранения материальных носителей персональных данных	Ответственное лицо
1	Республика Алтай, г. Горно-Алтайск, ул. Эркемена Палкина, 1, каб. 220	шкаф	Гелерт Альбина Оразбаевна, Сульянова Наталья Евгеньевна
2	Республика Алтай, г. Горно-Алтайск, ул. Эркемена Палкина, 1, каб. 221	сейф	Семенихина Татьяна Сергеевна, Черебеева Ижен Анатльевна
3	Республика Алтай, г. Горно-Алтайск, ул. Эркемена Палкина, 1, каб. 223	металлический шкаф с замком	Ялбакова Эркелей Дмитриевна
4	Республика Алтай, г. Горно-Алтайск, ул. Эркемена Палкина, 1, каб. 224	сейф	Панов Роман Владимирович
5	Республика Алтай, г. Горно-Алтайск, ул. Эркемена Палкина, 1, архивохранилище № 7	металлические стеллажи	Семенихина Татьяна Сергеевна, Черебеева Ижен Анатльевна
6	Республика Алтай, г. Горно-Алтайск, ул. В.И. Чаптынова, 28,	металлический шкаф с замком, сейф	Зорина Ольга Алексеевна, Майманова Светлана Пантелеевна,

	Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС г. Горно-Алтайска		Кресс Лариса Ивановна, Яжанкина Жанна Олеговна
7	Республика Алтай, Кош-Агачский район, с. Кош-Агач, ул. Пограничная, 13, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Кош-Агачского района	металлический шкаф с замком, сейф	Майхиева Лариса Олеговна, Бойдоева Айсура Эркеменовна
8	Республика Алтай, Майминский район, с. Майма, ул. Ленина, 22, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Майминского района	металлический шкаф с замком, сейф	Беловолова Елена Александровна, Шикакова Айана Григорьевна, Аргокова Алевтина Игнатьевна
9	Республика Алтай, Онгудайский район, с. Онгудай, ул. Советская, 78, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Онгудайского района	металлический шкаф с замком, сейф	Питеева Лариса Борисовна
10	Республика Алтай, Турочакский район, с. Турочак, ул.Советская, 77, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Турочакского района	металлический шкаф с замком, сейф	Чибисова Светлана Андреевна, Синкина Полина Андреевна
11	Республика Алтай, Улаганский район, с.Улаган, ул. Санаа, 8, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Улаганского района	металлический шкаф с замком, сейф	Герасимова Людмила Владимировна, Адагызова Валентина Валерьевна

12	Республика Алтай, Усть-Канский район, с. Усть-Кан, ул., Первомайская, 1, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Усть-канского района	металлический шкаф с замком, сейф	Карманова Карина Евгеньевна, Мюсова Арчынай Варельевна
13	Республика Алтай, Усть-Коксинский район, с. Усть-Кокса, ул. Харитошкина, 1А Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Усть-Коксинского района	металлический шкаф с замком, сейф	Чевалкова Любовь Алексеевна, Гавло Татьяна Васильевна
14	Республика Алтай, Чемальский район, с.Чемал, ул. Пчелкина, 83 Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Чемальского района	металлический шкаф с замком, сейф	Тенгерекова Инна Владимировна
15	Республика Алтай,Чойский район, с. Чоя, ул. Ленина, 27 Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Чойского района	металлический шкаф с замком, сейф	Штанова Валентина Константиновна
16	Республика Алтай, Шебалинский район, с. Шебалино, ул. Советская, 21, Комитет по делам ЗАГС и архивов Республики Алтай Отдел ЗАГС Шебалинского района	металлический шкаф с замком, сейф	Иркитова Анастасия Геннадьевна, Пшеничникова Наталья Евгеньевна

Приложение №19
К приказу Комитета
по делам ЗАГС и архивов
Республики Алтай
От 23.12.2020 № 94/1

Журнал учета запросов/обращений субъектов персональных данных

Начат «___» _____20___г.

Окончен «___» _____20___г.

Ответственный за ведение журнала _____

№ п/п	Дата обращения	ФИО субъекта	Данные субъекта (паспорт)	Цель запроса	Результат	Дата предоставления ответа и подпись