МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ КУЗБАССА (МИНЦИФРА КУЗБАССА)

ПРИКАЗ

от «08» декабря 2022 г. №135-п
г. Кемерово

Об утверждении документов по обработке и защите персональных данных в Министерстве цифрового развития и связи Кузбасса

Во исполнение «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», утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211, п р и к а з ы в а ю:

1. Утвердить прилагаемые документы:

1.1. Правила обработки персональных данных в Министерстве цифрового развития и связи Кузбасса, согласно приложению №1 к настоящему приказу.

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в Министерстве цифрового развития и связи Кузбасса согласно приложению №2 к настоящему приказу.

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных в Министерстве цифрового развития и связи Кузбасса требованиям к защите персональных данных согласно приложению № 3 к настоящему приказу.

1.4. Правила работы с обезличенными данными в Министерстве цифрового развития и связи Кузбасса согласно приложению № 4 к настоящему приказу.

1.5. Перечень информационных систем персональных данных Министерства цифрового развития и связи Кузбасса согласно приложению № 5 к настоящему приказу.

1.6. Перечень персональных данных, обрабатываемых в Министерстве цифрового развития и связи Кузбасса в связи с реализацией служебных и трудовых отношений, а также в связи с осуществлением государственных функций согласно приложению № 6 к настоящему приказу.

1.7. Перечень должностей государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению № 7 к настоящему приказу.

1.8. Перечень должностей, не являющихся должностями государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению №8 к настоящему приказу.

1.9. Перечень должностей государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению №9 к настоящему приказу.

1.10. Перечень должностей, не являющихся должностями государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению №10 к настоящему приказу.

1.11. Порядок доступа государственных гражданских служащих Кемеровской области – Кузбасса и работников, не являющихся государственными гражданскими служащими Кемеровской области – Кузбасса, в Министерстве цифрового развития и связи Кузбасса в помещения, в которых ведется обработка персональных данных согласно приложению №11 к настоящему приказу.

1.12. Перечень информационных систем персональных данных Министерства цифрового развития и связи Кузбасса, к которым осуществляется доступ государственных гражданских служащих Кемеровской области – Кузбасса и работников, не являющихся государственными гражданскими служащими Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, в рамках выполнения функций в установленной сфере деятельности согласно приложению №12 к настоящему приказу.

1.13. Перечень помещений Министерства цифрового развития и связи Кузбасса, в которых осуществляется обработка персональных данных согласно приложению №13 к настоящему приказу.

1.14. Форма перечня лиц, допущенных в помещения, в которых производится обработка персональных данных согласно приложению №14 к настоящему приказу.

1.15. Политика обеспечения безопасности персональных данных в информационных системах персональных данных Министерства цифрового развития и связи Кузбасса согласно приложению №15 к настоящему приказу.

1.16. Форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно приложению №16 к настоящему приказу.

1.17. Форма обязательства государственного гражданского служащего Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей согласно приложению №17 к настоящему приказу.

1.18. Форма обязательства лица, замещающего должность, не являющейся должностью государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей согласно приложению №18 к настоящему приказу.

1.19. Согласие на обработку персональных данных государственных гражданских служащих Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, а также иных субъектов персональных данных согласно приложению №19 к настоящему приказу.

2. Начальнику отдела информационной безопасности управления информационной безопасности и связи Министерства (С.С. Фомину) обеспечить:

2.1. Проведение не реже 1 раза в год обучения в Министерстве по вопросам исполнения требований документов, утверждаемых настоящим приказом.

2.2. Опубликование документов определяющих политику в отношении обработки персональных данных (настоящего приказа с приложениями № 1 - 15) на официальном сайте Министерства в сети «Интернет» в 10-дневный срок со дня подписания.

2.3. Проведение не реже 1 раза в полугодие проверки актуальности документов, утверждаемых настоящим приказом, и при необходимости внесение изменений.

2.4. Поддержание в актуальном состоянии сведений о Министерстве в реестре операторов, осуществляющих обработку персональных данных, размещенном на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в сети «Интернет».

3. Признать утратившим силу приказ Министерства цифрового развития и связи Кузбасса от 27 октября 2020 года № 144-п «Об утверждении документов по обработке и защите персональных данных в Министерстве цифрового развития и связи Кузбасса».

4. Контроль за исполнением настоящего приказа возложить на заместителя министра цифрового развития и связи Кузбасса - начальника управления информационной безопасности и связи Министерства цифрового развития и связи Кузбасса Утенкову О.М.

5. Настоящий приказ вступает в силу со дня подписания.

И.о. министра О.М. Утенкова

Приложение № 1
к приказу Министерства
цифрового развития
и связи Кузбасса
«08» декабря 2022 г. №135-п

Правила
обработки персональных данных
в Министерстве цифрового развития и связи Кузбасса

I. Общие положения

1. Настоящие Правила обработки персональных данных (далее – Правила) определяют цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Министерстве цифрового развития и связи Кузбасса (далее – Министерство).

2. Настоящие Правила определяют политику Министерства как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

3. Настоящие Правила разработаны в соответствии с:

Трудовым кодексом Российской Федерации (далее – Трудовой кодекс);

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

Федеральным законом от 27 мая 2003 г. № 58-ФЗ «О системе государственной службы Российской Федерации»;

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

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

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

Указом Президента Российской Федерации от 1 февраля 2005 г. № 112 «О конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации»;

Указом Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного

гражданского служащего Российской Федерации и ведении его личного дела»;

постановлением Губернатора Кемеровской области – Кузбасса от 23.12.2020 № 118-пг «О персональных данных государственного гражданского служащего Кемеровской области – Кузбасса и ведении его личного дела»;

постановлением 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»;

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

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

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

распоряжением Правительства Российской Федерации от 26 мая 2005 г. № 667-р;

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

приказом Федеральной службы по техническому и экспертному контролю от 11 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».

4. Обработка персональных данных в Министерстве осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных, а также настоящими Правилами.

II. Категории субъектов персональных данных

5. К субъектам персональных данных, персональные данные которых обрабатываются в Министерстве в соответствии с настоящими Правилами, относятся:

1) государственные гражданские служащие Кемеровской области – Кузбасса в Министерстве (далее – гражданские служащие Министерства);

2) граждане, претендующие на замещение должностей государственной гражданской службы в Министерстве;

3) работники Министерства, замещающие должности, не являющиеся должностями государственной гражданской службы Кемеровской области – Кузбасса (далее - работники Министерства);

4) граждане, претендующие на замещение должностей, не являющихся должностями государственной гражданской службы;

5) лица, состоящие в родстве (свойстве) с субъектами персональных данных, указанными в подпунктах 1-4 пункта 5 настоящих Правил;

6) лица, представляемые к награждению, наградные материалы по которым представлены в Министерство;

7) граждане, ранее трудоустроенные в Министерстве, работавшие в Министерстве на должностях гражданских служащих и должностях, не относящихся к должностям гражданских служащих и уволившиеся с работы по различным причинам;

8) физические лица и представители организаций, обратившиеся в Министерство в связи с исполнением функций, возложенных на Министерство;

9) граждане Российской Федерации и иностранных государств в соответствии с требованиями законодательства;

10) граждане, обратившиеся в Министерство в соответствии с Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»;

11) лица, замещающие должности руководителей организаций, подведомственных Министерству (далее - руководители организаций).

III. Условия и порядок обработки персональных данных субъектов персональных данных в связи с реализацией служебных или трудовых отношений

6. Персональные данные субъектов персональных данных (далее – персональные данные), указанных в подпунктах 1-7 пункта 5 настоящих Правил, обрабатываются в целях обеспечения задач кадровой работы, в том числе кадрового учета, делопроизводства, содействия в осуществлении служебной (трудовой) деятельности, формирования кадрового резерва, обучения и должностного роста, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности субъектов персональных данных, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, а также в целях противодействия коррупции.

7. В целях, указанных в пункте 6 настоящих Правил, обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

8. Согласие на обработку персональных данных субъекта персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, не требуется при обработке персональных данных в соответствии с Федеральным законом «О персональных данных».

9. Согласие на обработку специальных категорий персональных данных, а также биометрических персональных данных субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, не требуется при обработке персональных данных в соответствии с Федеральным законом «О персональных данных» и положениями Трудового кодекса, за исключением случаев получения персональных данных работника у третьей стороны.

10. Необходимо получить согласие субъекта персональных данных на обработку его персональных данных в следующих случаях:

при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о государственной гражданской службе и о противодействии коррупции;

при трансграничной передаче персональных данных;

при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

11. В случаях, предусмотренных пунктом 10 настоящих Правил, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

При оформлении согласия, субъект персональных данных разрешает / не разрешает:

- фамилию, имя, отчество (при наличии) использовать в качестве общедоступных в электронной почте и системе электронного документооборота Министерства и Администрации Правительства Кузбасса, а также в иных случаях, предусмотренных законодательством Российской Федерации об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления;

- дату рождения (число, месяц и год рождения) и фотографию использовать в качестве общедоступных для публикации на внутренних информационных ресурсах и на официальных сайтах Администрации Правительства Кузбасса и Министерства, а также в иных случаях, предусмотренных законодательством Российской Федерации об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления.

12. Обработка персональных данных субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, осуществляется гражданским служащим кадровой службы в Министерстве (далее - уполномоченный сотрудник кадровой службы).

13. Обработка персональных данных субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, включает в себя следующие действия: сбор (получение), запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

14. Сбор (получение), запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, осуществляется путем:

получения оригиналов необходимых документов;

копирования оригиналов документов;

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

формирования персональных данных в ходе кадровой работы;

внесения персональных данных в автоматизированные информационные системы, оператором которых является Министерство и/или Администрация Правительства Кузбасса и/или Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее - автоматизированные информационные системы), используемые в целях кадровой работы.

15. Сбор (получение), запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил.

16. В случае возникновения необходимости получения персональных данных субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, у третьей стороны, следует известить об этом субъектов персональных данных заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

17. Запрещается получать, обрабатывать и приобщать к личным делам гражданских служащих и работников Министерства, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, частной жизни, членства в общественных объединениях.

18. При сборе персональных данных уполномоченный сотрудник кадровой службы, осуществляющий сбор (получение) персональных данных непосредственно от субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

19. Передача (распространение, предоставление) и использование персональных данных субъектов персональных данных, чьи данные обрабатываются в целях, определенных пунктом 6 настоящих Правил, осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

IV. Условия и порядок обработки персональных данных гражданских служащих Министерства и лиц, состоящих с ними в родстве (свойстве), в связи с рассмотрением заявлений на получение долгосрочных целевых жилищных займов и социальных выплат на приобретение жилых помещений

20. В Министерстве осуществляется обработка персональных данных гражданских служащих Министерства и лиц, замещающих должности, не отнесенные к должностям государственной гражданской службы Кемеровской области - Кузбасса в Министерстве и лиц, состоящих с ними в родстве (свойстве), в связи с рассмотрением заявлений на получение долгосрочных целевых жилищных займов и социальных выплат на приобретение жилых помещений (далее - займ).

21. В связи с рассмотрением вопроса о предоставлении займа подлежат обработке следующие персональные данные:

1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена, отчества (при наличии) в случае их изменения);

2) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при его наличии), выдавшего его, дата выдачи;

3) адрес и дата регистрации (снятия с регистрационного учета) по месту жительства (месту пребывания);

4) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших мужьях (женах);

5) персональные данные, содержащиеся в выписке из домовой книги, копиях финансового лицевого счета, свидетельства о браке, свидетельства о рождении ребенка (детей), трудовой книжки, документов о наличии в собственности гражданского служащего Министерства и (или) членов его семьи жилых помещений, кроме жилого помещения, в котором они зарегистрированы (с предоставлением при необходимости их оригиналов), документа, подтверждающего право на дополнительную площадь жилого помещения (в случаях, когда такое право предоставлено законодательством Российской Федерации);

6) иные персональные данные, ставшие известными в связи с рассмотрением вопроса о предоставлении займа.

22. Обработка персональных данных гражданских служащих Министерства и лиц, замещающих должности, не отнесенные к должностям государственной гражданской службы Министерства и лиц, состоящих с ними в родстве (свойстве), при постановке на учет для получения займа осуществляется на основании заявления, представляемого на имя Министра

цифрового развития и связи Кузбасса в комиссию по рассмотрению заявлений на получение долгосрочных целевых жилищных займов и социальных выплат на приобретение жилых помещений (далее – Комиссия по предоставлению займов).

23. Обработка персональных данных гражданских служащих Министерства и лиц, замещающих должности, не отнесенные к должностям государственной гражданской службы Кемеровской области - Кузбасса Министерства и лиц, состоящих с ними в родстве (свойстве), в связи с предоставлением займа, в частности, сбор (получение), запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется государственными гражданскими служащими Кемеровской области – Кузбасса Министерства, входящими в состав Комиссии по предоставлению займов, путем:

1) получения оригиналов необходимых документов;

2) предоставления заверенных в установленном законодательством Российской Федерации порядке копий документов.

24. Комиссия по предоставлению займов вправе проверять сведения, содержащиеся в документах, представленных государственными гражданскими служащими Кемеровской области – Кузбасса и лицами, замещающих должности, не отнесенные к должностям государственной гражданской службы Кемеровской области - Кузбасса Министерства о наличии условий, необходимых для постановки гражданского служащего Министерства на учет для получения займа.

25. Передача (распространение, предоставление) и использование персональных данных государственных гражданских служащих Кемеровской области – Кузбасса и лиц, замещающих должности, не отнесенные к должностям государственной гражданской службы Кемеровской области - Кузбасса Министерства и лиц, состоящих с ними в родстве (свойстве), полученных в связи с предоставлением субсидии, осуществляется в случаях и в порядке, предусмотренных законодательством Российской Федерации.

V. Условия и порядок обработки персональных данных субъектов персональных данных в связи с исполнением функций, возложенных на Министерство

26. В Министерстве обработка персональных данных физических лиц и представителей организаций (далее – заявители) осуществляется в связи с:

1) обработкой входящей и исходящей корреспонденции, содержащей персональные данные (в т.ч. допуск граждан в рамках государственных контрактов) производится обработка персональных данных должностных лиц организаций и граждан,

2) ведением бухгалтерского учета,

3) оформлением трудовых отношений при поступлении на государственную службу Кемеровской области - Кузбасса в Министерство цифрового развития и связи Кузбасса, участием граждан в конкурсах для

включения в кадровый резерв государственной гражданской службы Кемеровской области – Кузбасса и кадровый резерв государственной гражданской службы Кемеровской области – Кузбасса,

4) оформлением допуска к государственной тайне,

5) ведения воинского учета и бронирования,

6) оформлением электронных пропусков на время действия режима повышенной готовности в Кузбассе,

7) поиска, регистрации, подтверждения, удаления, восстановление учетных записей пользователей единой системы идентификации и аутентификации в приложении «Центр обслуживания ЕСИА» (АРМ Центра обслуживания Госуслуги),

8) обеспечением деятельности по защите информации производится обработка персональных данных государственных гражданских служащих Кемеровской области - Кузбасса и работников, не являющихся государственными гражданскими служащими Кемеровской области - Кузбасса, Министерства и должностных лиц организаций в объеме, необходимом для проведения мероприятий по защите информации, обрабатываемой в информационных системах Министерства,

9) обеспечением своевременного и в полном объеме рассмотрения устных и письменных обращений граждан Российской Федерации в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

27. В целях, указанных в пункте 26 настоящих Правил, осуществляется обработка персональных данных заявителей, в соответствии с требованиями каждой цели.

28. Обработка персональных данных в целях, указанных в пункте 26 настоящих Правил, осуществляется соответствующими подразделениями Министерства, в положения об отделах, которых входит исполнение тех или иных функций, возложенных на Министерство.

29. Сбор (получение), запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в целях, указанных в пункте 26 настоящих Правил, осуществляется путем:

получения оригиналов необходимых документов (заявлений);

заверения копий документов;

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

внесения персональных данных в автоматизированные информационные системы.

30. Сбор (получение), запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от заявителей.

31. Запрещается запрашивать у заявителей и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

32. Передача (распространение, предоставление) и использование персональных данных заявителей осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

VI. Условия и порядок обработки персональных данных субъектов персональных данных в связи с рассмотрением обращений граждан

33. В Министерстве обработка персональных данных граждан осуществляется в целях обеспечения своевременного и в полном объеме рассмотрения их устных и письменных обращений в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

34. Персональные данные граждан, обратившихся в Министерство лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением граждан о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в Министерстве подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

35. В соответствии с Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации» в связи с рассмотрением поступивших в Министерстве обращений граждан обработке подлежат следующие персональные данные:

1) фамилия, имя, отчество (при наличии);

2) почтовый адрес;

3) адрес электронной почты;

4) указанный в обращении контактный телефон;

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

36. Обработка персональных данных, необходимых в связи с рассмотрением обращений граждан, осуществляется без согласия субъектов персональных данных в соответствии с Федеральным законом «О персональных данных» и Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

37. Передача (распространение, предоставление) и использование персональных данных, указанных в пункте 35 настоящих Правил, осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

VII. Порядок обработки персональных данных в автоматизированных информационных системах

38. Обработка персональных данных в Министерстве может осуществляется с использованием автоматизированных информационных систем.

Перечень автоматизированных информационных систем утверждается приказом Министерства.

39. Доступ к автоматизированным информационным системам государственных гражданских служащих и работников Министерства, осуществляющих обработку персональных данных в автоматизированных информационных системах, реализуется посредством учетной записи, состоящей из имени пользователя и пароля.

40. Доступ к автоматизированным информационным системам предоставляется в соответствии с функциями, предусмотренными должностными регламентами гражданских служащих и работников Министерства, на основании Перечня работников Министерства цифрового развития и связи Кузбасса (пользователей средств криптографической защиты информации), допущенных к сбору, хранению и обработке информации, содержащей сведения ограниченного доступа, не содержащие сведения, составляющих государственную тайну, (конфиденциального характера), и имеющих полномочия на подписание электронных документов и соответствующих списков, предусмотренных Мероприятиями по организации допуска работников Министерства, допущенных к сбору, хранению и обработке информации, содержащей сведения ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера), наделению полномочиями для подписания электронных документов.

41. Информация может размещаться в автоматизированных информационных системах как в автоматическом, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

42. Обеспечение безопасности персональных данных, обрабатываемых в автоматизированных информационных системах, осуществляется отделом информационной безопасности и достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных согласно Федеральному закону «О персональных данных».

VIII. Организация хранения персональных данных

43. Персональные данные хранятся на бумажных носителях в структурных подразделениях Министерства.

44. Персональные данные хранятся в электронном виде в автоматизированных электронных системах.

45. Хранение документов осуществляется раздельно, исходя из цели обработки персональных данных. Места хранения персональных данных (материальных носителей) в структурных подразделениях Министерства определяют начальники структурных подразделений, в которых производится обработка персональных данных. Хранение персональных данных на бумажных носителях информации и съемных носителях информации осуществляется в сейфах или шкафах, опечатываемых личными печатями ответственных лиц.

46. Архивное хранение документов и информации на машинных носителях информации осуществляется в помещениях (архивах) предназначенных для данных целей, ответственным за ведение архива Министерства, назначенным приказом Министерства.

47. Сроки хранения персональных данных на бумажном носителе определяются нормативными правовыми актами, регламентирующими порядок их сбора (получения) и обработки.

48. Срок хранения персональных данных, внесенных в автоматизированные информационные системы, должен соответствовать сроку хранения персональных данных на бумажных носителях.

49. Уточнение сроков хранения документов осуществляется экспертной комиссией, созданной приказом Министерства.

50. Персональные данные при их обработке, осуществляемой без использования автоматизированных информационных систем, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

51. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях персональных данных, обработка которых осуществляется в целях, определенных настоящими Правилами.

IX. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

52. Документы, содержащие персональные данные, сроки хранения которых истекли, подлежат уничтожению.

53. Документы, содержащие персональные данные, на бумажном носителе передаются в помещения для хранения архива Министерства для уничтожения в порядке, установленном законодательством Российской Федерации об архивном деле и правовым актом Министерства.

54. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

X. Порядок доступа в помещения, в которых ведется обработка персональных данных

55. Порядок доступа в помещения, в которых ведется обработка персональных данных, утверждается приказом Министерства.

XI. Ответственный за организацию обработки персональных данных

56. Ответственный за организацию обработки персональных данных в Министерства (далее - ответственный за обработку персональных данных), назначается приказом Министерства.

57. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных, настоящими Правилами и должностной инструкцией ответственного за организацию обработки персональных данных в Министерстве цифрового развития и связи Кузбасса, утверждаемой приказом Министерства.

Приложение № 2
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Правила рассмотрения запросов субъектов персональных данных или их представителей в Министерстве цифрового развития и связи Кузбасса

1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) разработаны в соответствии с требованиями 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, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211.

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

1.3. Субъект персональных данных имеет право доступа к своим персональным данным, обработка и хранение которых осуществляется в Министерстве цифрового развития и связи Кузбасса (далее – Министерство).

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

- подтверждение факта обработки персональных данных Министерства;
- правовые основания и цели обработки персональных данных;
- цели и способы обработки персональных данных, применяемые Министерством;
- обрабатываемые персональные данные, относящиеся к субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен действующим законодательством;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством Российской Федерации;
- информацию о проведенной или о предполагаемой трансграничной передаче данных;

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

- иные сведения, предусмотренные федеральными законами и нормативными правовыми актами.

1.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с действующим законодательством.

1.6. Субъект персональных данных вправе требовать от Министерства 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 иные предусмотренные законом меры по защите своих прав.

1.7. Копии документов, не относящиеся к трудовой деятельности (например, паспорт, свидетельство о рождении, свидетельство о заключении брака, свидетельство о расторжении брака, диплом об образовании, военный билет, полис обязательного медицинского страхования, страховое свидетельство обязательного пенсионного страхования, свидетельство о постановке на учет в налоговом органе (идентификационный номер налогоплательщика) субъекту персональных данных оператором не выдаются.

1.8. Сведения, указанные в п.1.4 настоящих Правил, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

1.9. Сведения, указанные в п. 1.4, настоящих Правил предоставляются субъекту персональных данных или его представителю при обращении, либо при получении Министерством запроса субъекта персональных данных или его законного представителя.

Запрос должен содержать сведения, в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», типовая форма запроса приведена в приложении № 1.

При получении запроса от законного представителя субъекта персональных данных, к запросу должен быть приложен документ (заверенный в соответствии требованиями действующего законодательства), подтверждающий право представителя получать персональные данные субъекта персональных данных. В случае отсутствия указанного документа, Министерство вправе мотивировано отказать в приеме запроса.

1.10. Если субъекту персональных данных, по его запросу, были предоставлены для ознакомления запрашиваемые персональные данные, то субъект персональных данных вправе обратиться повторно или направить повторный запрос не ранее чем через тридцать дней после первоначального

обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

1.11. Субъект персональных данных вправе обратиться повторно или направить повторный запрос в целях получения сведений, до истечения срока, указанного в п.1.10, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос, должен содержать обоснование направления повторного запроса.

1.12. Министерство вправе отказать субъекту персональных данных в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Министерстве.

1.13. Регистрация и исполнение запросов субъектов персональных данных, являющихся гражданскими государственными служащими (далее – служащие) или работниками, не являющимися государственными гражданскими служащими (далее – работники), Министерства на предоставление копии трудовой книжки осуществляется специалистом кадровой службы.

1.14. Регистрация и исполнение запросов субъектов персональных данных, являющихся служащими или работниками Министерства на предоставление справок по форме 2-НДФЛ осуществляется специалистом бухгалтерии.

1.15. Запросы субъектов персональных данных, являющихся служащими или работниками Министерства, на предоставление документов, не указанных в п.1.13 и п.1.14, и ответы на запросы регистрируются ответственным служащим или работником за регистрацию входящей корреспонденции в сроки, установленные действующим законодательством Российской Федерации.

1.16. Запросы субъектов персональных данных, полученные от граждан, не являющихся служащими или работниками Министерства и ответы на указанные запросы, регистрируются ответственным служащим или работником за регистрацию входящей корреспонденции в сроки, установленные действующим законодательством Российской Федерации.

1.17. Обработка документов, содержащих персональные данные субъектов, разрешена только служащим или работникам Министерства, допущенных к обработке персональных данных.

1.18. Служащий или работник Министерства, которому в соответствии с решением Министра цифрового развития и связи Кузбасса (лица его замещающего), направлен запрос субъекта персональных данных для исполнения, несет персональную ответственность за неразглашение

персональных данных, выполнение требований действующего законодательства и нормативных правовых актов по защите персональных данных, при обработке запроса субъекта персональных данных и подготовке ответа на указанный запрос.

1.19. Запрос субъекта персональных данных (его представителя) рассматривается в установленные сроки в соответствии с действующим законодательством Российской Федерации.

2. Правила рассмотрения запросов субъектов персональных данных или их представителей

2.1. Субъект персональных данных может обратиться с запросом в Министерство в следующей форме:

- письменно (запрос напечатан или написан от руки на бумаге), путем направления письма почтовой связью или путем подачи запроса в Министерство лично или через своего представителя;
- в форме электронного документа, подписанного электронной подписью в соответствии с требованиями действующего законодательства Российской Федерации;
- в устной форме в соответствии с требованиями действующего законодательства Российской Федерации.

2.2. Письменный запрос поступает почтой или предоставляется лично субъектом персональных данных (представителем субъекта персональных данных) в Министерство или через приемную обращений граждан Администрации Правительства Кузбасса.

2.2.1. Ответственный служащий или работник при получении запроса обязан зарегистрировать запрос субъекта персональных данных, обработать его в соответствии установленными в Министерстве требованиями к делопроизводству и передать исполнителю.

2.2.2. Исполнитель соответствующего отдела, которому направлен документ для исполнения, обязан на своем автоматизированном рабочем месте подготовить ответ на полученный запрос, после чего обеспечить дальнейшее его направление в соответствии с установленными в исполнительных органах государственной власти требованиями к делопроизводству.

2.2.3. Служащий или работник, ответственный за регистрацию и отправку исходящей корреспонденции, при получении ответа на запрос субъекта персональных данных обязан зарегистрировать полученный документ и отправить документ субъекту персональных данных.

2.3. Запрос субъекта персональных данных (его представителя) может поступить в Министерство или через приемную обращений граждан Администрации Правительства Кузбасса в виде электронного документа с электронной подписью в соответствии с действующим законодательством Российской Федерации.

Прием запросов субъектов персональных данных осуществляет уполномоченный служащий или работник, на которого возложены обязанности по приему и обработке входящей корреспонденции. Для проверки наличия и достоверности электронной подписи могут привлекаться служащие отдела информационной безопасности.

2.3.1. Уполномоченный служащий или работник, ответственный за получение и регистрацию входящей корреспонденции, при получении запроса субъекта персональных данных, обязан:

- проверить подлинность электронной подписи субъекта персональных данных с привлечением, в случае необходимости, сотрудника отдела информационной безопасности, являющегося администратором информационной безопасности Министерства;
- зарегистрировать запрос субъекта персональных данных, обработать его в соответствии с установленными в Министерстве требованиями к делопроизводству и передать исполнителю.

2.3.2. Исполнитель при получении запроса субъекта персональных данных в электронном виде выполняет действия, указанные в п.2.2.2 настоящих Правил.

2.3.3. Субъект персональных данных несет персональную ответственность за хранение и правомерное использование своих закрытых ключей электронной подписи.

2.4. Исполнителям разрешено производить обработку информации, содержащей персональные данные субъекта, только на специально выделенных защищенных информационных ресурсах.

2.5. Исполнителям запрещается копировать файл подготовленного ответа на запрос субъекта персональных данных на съемные машинные носители информации и общедоступные информационные ресурсы Министерства.

2.6. Исполнители несут полную ответственность при обработке персональных данных в соответствии с действующим законодательством Российской Федерации.

2.7. В случае направления исполнителем уведомления об уничтожении персональных данных субъекта персональных данных необходимо руководствоваться формой уведомления (приложение № 2).

Приложение № 1
к Правилам рассмотрения запросов
субъектов персональных данных
«08» декабря 2022 г. №135-п

Типовая форма запроса субъекта персональных данных на доступ к своим персональных данным

В Министерство цифрового
развития и связи Кузбасса

от_____
(ФИО заявителя)

_____

адрес:_____

_____

паспорт серия _____ № _____
выдан _____

_____

_____

телефон _____
e-mail: _____

ЗАЯВЛЕНИЕ

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, а также:

– указать основания, цели и источник получения такой информации;

– указать способы и сроки ее обработки (в том числе сроки хранения);

– предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ) на основании договора с Министерством цифрового развития и связи Кузбасса или на основании федерального закона;

– предоставить информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– указать наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Министерства цифрового развития и связи Кузбасса, если обработка поручена или будет поручена такому лицу;

– предоставить сведения о том, какие юридические последствия для меня может повлечь её обработка.

В случае отсутствия такой информации прошу Вас уведомить меня об этом.

_____ _____

(подпись) *(ФИО)*

___ _____20__ г.

Приложение № 2
к Правилам рассмотрения запросов
«08» декабря 2022 г. №135-п

ФОРМА УВЕДОМЛЕНИЯ
об уничтожении персональных данных

Бланк Министерства

Уведомление

Настоящим уведомлением сообщаем Вам, что в соответствии с требованиями статьи 21 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», Ваши персональные данные в информационной системе персональных данных «указать наименование информационной системы» уничтожены.

_____	_____	_____
(должность)	*(подпись)*	*(расшифровка подписи)*

Приложение № 3
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Правила
осуществления внутреннего контроля соответствия обработки персональных данных в Министерстве цифрового развития и связи Кузбасса требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в Министерстве цифрового развития и связи Кузбасса требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Министерства цифрового развития и связи Кузбасса (далее - Правила), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных) в Министерстве цифрового развития и связи Кузбасса (далее – Министерство).

2. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона «О персональных данных».

3. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Министерстве организовывается проведение периодических проверок условий обработки персональных данных (далее - проверки).

4. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в Министерстве (далее - ответственный за организацию обработки персональных данных), либо комиссией, образуемой приказом Министерства.

В проведении проверки не может участвовать служащий Министерства, прямо или косвенно заинтересованный в ее результатах.

5. Проверки проводятся на основании утвержденного министром цифрового развития и связи Кузбасса плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных (плановые проверки) или на основании поступившего в Министерство письменного заявления о

нарушениях правил обработки персональных данных (внеплановые проверки).

6. Проведение внеплановой проверки организуется в течение семи рабочих дней с момента поступления в Министерство соответствующего заявления.

7. При проведении проверки 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.

8. Ответственный за организацию обработки персональных данных или комиссия имеет право:

запрашивать у работников Министерства информацию, необходимую для реализации полномочий;

требовать от лиц, уполномоченных на обработку персональных данных в Министерстве 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;

вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства о персональных данных.

9. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Министерстве либо комиссии в ходе проведения мероприятий внутреннего

контроля, должна обеспечиваться конфиденциальность персональных данных.

10. По результатам проведения проверки оформляется протокол проведения внутренней проверки условий обработки ПДн (приложение № 1), который подписывается ответственным за организацию обработки персональных данных или членами комиссии, а также руководителем (ответственным) проверяемого подразделения. Допускается оформление документа в электронном виде, в таком случае документ подписывается квалифицированными электронными подписями в системе электронного документооборота.

Срок проведения проверки и оформления протокола составляет тридцать календарных дней со дня начала проверки, указанного в правовом акте о назначении проверки.

11. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных либо председатель комиссии информирует министра цифрового развития и связи Кузбасса или лицо его замещающее по форме приложения № 2.

Приложение №1
к Правилам осуществления
внутреннего контроля
«08» декабря 2022 г. №135-п

ФОРМА ПРОТОКОЛА
проведения внутренней проверки условий обработки персональных данных в Министерстве цифрового развития и связи Кузбасса

Настоящий Протокол составлен в том, что «___» _____ 20__ г. ответственным за организацию обработки ПДн (членами комиссии, назначенной приказом …) проведена проверка _____.
(тема проверки)

Проверка осуществлялась в соответствии с требованиями:
_____
_____
_____.
(название документа)

В ходе проверки проверено:
_____
_____
_____
_____
_____
_____.

Выявленные нарушения:
_____
_____
_____
_____
_____
_____
_____.

Меры по устранению нарушений:
_____
_____
_____
_____

_____
_____
_____.

Срок устранения нарушений: _____.

Должность ответственного за организацию обработки ПДн, подпись:
_____ *И.О. Фамилия*

Должность руководителя(ответственного) проверяемого подразделения, подпись:
_____ *И.О. Фамилия*

Члены комиссии:

Должность, подпись
_____ *И.О. Фамилия*

Должность, подпись
_____ *И.О. Фамилия*

Приложение № 2
к Правилам осуществления
внутреннего контроля
«08» декабря 2022 г. №135-п

ТИПОВАЯ ФОРМА УВЕДОМЛЕНИЯ
о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений

Настоящим уведомлением сообщаем Вам, что при проведении проверки условий обработки персональных данных на объекте информатизации «*указать наименование объекта (ГИС, ИСПДн. АРМ и т.п.*):

В ходе проверки проверено:

_____
_____
_____.

Выявленные нарушения:

_____
_____
_____.

Приняты следующие меры по устранению нарушений:

_____
_____
_____
_____.

По состоянию на _____ все нарушения устранены.

_____	_____	_____
(должность)	*(подпись)*	*(расшифровка подписи)*

___ _____20___г.

Приложение № 4
к приказу Министерства
цифрового развития и связи
Кузбасса
«*08*» декабря 2022 г. №*135*-п

Правила работы с обезличенными данными в Министерстве цифрового развития и связи Кузбасса

I. Общие положения

1. Настоящие Правила работы с обезличенными данными (далее – Правила) в Министерстве цифрового развития и связи Кузбасса (далее – Министерство) определяют порядок работы в случае обезличивания персональных данных и разработаны в соответствии с:

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

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

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

приказом Федеральной службы по техническому и экспертному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – приказ ФСТЭК России № 17);

приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (далее – приказ Роскомнадзора № 996).

II. Порядок работы с обезличенными персональными данными

2. Обезличивание персональных данных в Министерстве проводится в статистических или иных исследовательских целях, а также с целью снижения ущерба от разглашения защищаемых персональных данных, снижения класса автоматизированных информационных систем, оператором которых является Министерство (далее - автоматизированные

информационные системы) и по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей.

3. Обезличиванию подвергаются персональные данные, обработка которых осуществляется в автоматизированных информационных системах.

4. Обезличивание персональных данных, обрабатываемых в автоматизированных информационных системах, осуществляется методами, определенными приказом Роскомнадзора № 996.

5. В процессе реализации процедуры обезличивания персональных данных следует соблюдать требования, предъявляемые к выбранному методу обезличивания, установленные приказом Роскомнадзора № 996.

6. До начала обезличивания персональных данных приказом Министерства утверждается Перечень государственных гражданских служащих Кемеровской области – Кузбасса в Министерстве (далее - гражданские служащие Министерства), ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных и возлагаются обязанности по обезличиванию персональных данных.

7. В случае необходимости обезличивания персональных данных, обрабатываемых в автоматизированных информационных системах, отдела Министерства, непосредственно осуществляющие обработку персональных данных, осуществляют подготовку предложений по обезличиванию персональных данных с обоснованием необходимости и метода обезличивания персональных данных и направляют указанную информацию в отдел информационной безопасности (далее - ОИБ) Министерства в форме служебной записки, подписанной начальником соответствующего отдела Министерства (уполномоченным им лицом) для подготовки приказа указанного в п.6 настоящего приказа.

8. Обезличивание персональных данных обеспечивается сотрудниками, назначенными приказом Министерства, методами, согласованными с ОИБ.

9. Обработка обезличенных персональных данных может осуществляться на бумажных носителях без использования средств автоматизации, а также в автоматизированных информационных системах в соответствии с инструкциями Министерства.

10. При обработке обезличенных персональных данных в автоматизированных информационных системах необходимо соблюдение:

парольной защиты автоматизированных информационных систем;

антивирусной политики;

правил работы со съемными носителями (в случае их использования);

правил резервного копирования;

правил доступа в помещения, где расположены элементы автоматизированных информационных систем.

11. При хранении обезличенных персональных данных следует:

организовать раздельное хранение обезличенных персональных данных и дополнительной (служебной) информации о выбранном методе

обезличивания персональных данных и параметрах процедуры обезличивания персональных данных;

обеспечивать конфиденциальность дополнительной (служебной) информации о выбранном методе обезличивания персональных данных и параметрах процедуры обезличивания персональных данных.

12. При обработке обезличенных персональных данных в автоматизированных информационных системах обеспечивается соблюдение требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации № 1119, а также организационно-технических мер по обеспечению безопасности персональных данных, определенных приказом ФСТЭК России № 17, с учетом уровней защищенности персональных данных, определенных Управлением для автоматизированных информационных систем, в которых осуществляется обработка персональных данных.

Приложение № 5
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. № 135-п

Перечень информационных систем персональных данных Министерства цифрового развития и связи Кузбасса

1. 1С:Предприятие 8. «Бухгалтерия»
2. 1С:Предприятие 8. «Зарплата и кадры государственного учреждения»
3. ИСПДн «Региональный реестр государственных услуг»
4. Официальный сайт Министерства цифрового развития и связи Кузбасса (https://digital42.ru)
5. Автоматизированная информационная система «Производственно-управленческая система Кузбасса» (ПУСК)

Приложение № 6
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень персональных данных, обрабатываемых в Министерстве цифрового развития и связи Кузбасса в связи с реализацией служебных и трудовых отношений, а также в связи с осуществлением государственных функций

1. Фамилия, имя, отчество, дата и место рождения, гражданство.
2. Прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения).
3. Владение иностранными языками и языками народов Российской Федерации.
4. Образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому).
5. Послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов).
6. Выполняемая работа с начала трудовой деятельности.
7. Классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы, классный чин юстиции (кем и когда присвоены).
8. Государственные награды, иные награды и знаки отличия (кем награжден и когда).
9. Степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены).
10. Места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены).
11. Фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен).
12. Пребывание за границей (когда, где, с какой целью).
13. Близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей).
14. Адрес и дата регистрации по месту жительства (месту пребывания),

адрес фактического проживания.

15. Паспорт (серия, номер, кем и когда выдан).

16. Паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, когда и кем выдан).

17. Свидетельства о государственной регистрации актов гражданского состояния.

18. Номера контактных телефонов (домашний, служебный, мобильный).

19. Отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу).

20. Идентификационный номер налогоплательщика.

21. Номер страхового свидетельства обязательного пенсионного страхования.

22. Реквизиты страхового медицинского полиса обязательного медицинского страхования, содержащиеся в нем сведения.

23. Наличие (отсутствие) судимости.

24. Допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата).

25. Наличие (отсутствие) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, подтвержденного заключением медицинского учреждения.

26. Результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования.

27. Сведения об инвалидности, сроке действия установленной инвалидности.

28. Фотография.

29. Сведения о доходах, о расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей.

30. Сведения о последнем месте государственной или муниципальной службы.

31. Табельный номер (лицевой счет).

32. Информация о приеме, переводе, увольнении и иных событиях, относящиеся к гражданской службе (трудовой деятельности) в Министерстве.

33. Сведения о доходах в Министерстве и предыдущих местах работы и доходах с предыдущих мест работ.

34. Номера банковских счетов.

35. Номера банковских пластиковых карт.

36. Иные сведения, которые субъект персональных данных пожелал сообщить о себе.

Приложение № 7
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень должностей государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Министр;
2. Заместитель министра;
3. Заместитель министра – начальник управления;
4. Начальник управления;
5. Начальник отдела;
6. Главный консультант;
7. Главный консультант – главный бухгалтер;
8. Ведущий консультант;
9. Консультант;
10. Консультант-юрисконсульт;
11. Главный специалист.

Приложение № 8
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень должностей, не являющихся должностями государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Методист;
2. Старший методист.

Приложение № 9
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень должностей государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Министр;
2. Заместитель министра;
3. Заместитель министра – начальник управления;
4. Начальник управления;
5. Начальник отдела;
6. Главный консультант;
7. Главный консультант – главный бухгалтер;
8. Ведущий консультант;
9. Консультант;
10. Консультант-юрисконсульт;
11. Главный специалист.

Приложение № 10
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень должностей, не являющихся должностями государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Методист;
2. Старший методист.

Приложение № 11
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Порядок доступа государственных гражданских служащих Кемеровской области – Кузбасса и работников, не являющихся государственными гражданскими служащими Кемеровской области – Кузбасса, в Министерстве цифрового развития и связи Кузбасса в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа государственных гражданских служащих Кемеровской области - Кузбасса (далее – служащие) и работников, не являющихся государственными гражданскими служащими Кемеровской области - Кузбасса (далее – работники), Министерства цифрового развития и связи Кузбасса (далее – Министерство) в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012г. №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», Положением о пропускном и внутриобъектовом режиме в зданиях Администрации Правительства Кузбасса.

2. Настоящий порядок разработан в целях определения правил доступа в помещения, в которых ведется обработка персональных данных.

3. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях.

Сдачу (вскрытие) помещения под охрану осуществляют служащие и работники Министерства, работающие в данном помещении или начальник отдела (лицо его замещающее).

При сдаче помещения под охрану служащие и работники Министерства, обязаны выполнить следующие мероприятия:

- убрать документы с персональными данными в сейфы (запирающиеся шкафы) и опечатать их личной печатью;
- выключить установленным порядком компьютерную технику и оргтехнику;
- закрыть окна;

- выключить электроприборы;
- выключить свет;
- закрыть входную дверь на замок и опечатать дверь помещения личной печатью;
- сделать запись в журнале приема-сдачи служебных помещений под охрану.

При вскрытии помещения, в котором ведется обработка персональных данных, служащие и работники министерства, вскрывающие помещение обязаны выполнить следующие мероприятия:

- сделать запись в журнале приема-сдачи помещений под охрану;
- проверить целостность печати на входной двери помещения;
- вскрыть помещение;
- проверить целостность печатей на сейфах (шкафах), наличие и целостность компьютерной и оргтехники;
- при обнаружении нарушения целостности печатей, отсутствии или целостности компьютерной техники, других нарушениях служащий или работник Министерства, вскрывающий помещение, в котором ведется обработка персональных данных, обязан доложить о выявленных нарушениях своему начальнику отдела (лицу его замещающему) и начальнику отдела данных и информационной безопасности (лицу его замещающему).

4. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются служащие или работники Министерства, уполномоченные на обработку персональных данных приказом Министерства.

6. Служащие или работники Министерства, осуществляющие обработку персональных данных до завершения рабочего дня обязаны вернуть носители персональных данных в помещения, где осуществляется их хранение.

7. Ответственными за организацию доступа в помещения Министерства, в которых ведется обработка и хранение персональных данных, являются начальники отделов Министерства или работники (служащие), не принадлежащие к отделам управлений Министерства.

8. Работники сторонних организаций, прибывшие в помещение, в котором ведется обработка персональных данных, для выполнения работ в соответствии с заключенным Министерством договором (контрактом) допускаются в помещение в присутствии служащих или работников, данного помещения.

9. При проведении таких работ, служащие или работники Министерства обязаны принять меры по исключению ознакомления

работников сторонних организаций с персональными данными.

10. Работники контролирующих органов, допускаются в помещение, в котором ведется обработка персональных данных, при наличии соответствующего предписания на проведение контрольных мероприятий, с разрешения министра цифрового развития и связи Кузбасса (лица его замещающего), в присутствии начальника отдела (лица его замещающего). Ознакомление с персональными данными лиц, прибывших для проведения контрольных мероприятий, осуществляется в объеме, предусмотренном планом проверки.

Приложение № 12
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень информационных систем персональных данных Министерства цифрового развита и связи Кузбасса, к которым осуществляется доступ государственных гражданских служащих Кемеровской области – Кузбасса и работников, не являющихся государственными гражданскими служащими Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, в рамках выполнения функций в установленной сфере деятельности

1. «Государственная информационная система о государственных и муниципальных платежах».
2. «Государственная интегрированная информационная система управления общественными финансами «Электронный бюджет».
3. «Информационная система Удостоверяющего центра Федерального казначейства».
4. Система удаленного финансового документооборота «Автоматизированной системы Федерального казначейства».
5. Единая информационная система управления кадровым составом государственной гражданской службы РФ (ЕИСУ КС).
6. Федеральный ситуационный центр электронного правительства.
7. Система справочного телефонного узла Администрации Президента Российской Федерации.
8. АРМ Центра обслуживания (сервис).
9. АРМ заказчика.
10. «Единое окно цифровой обратной связи Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг».
11. Система «Контур.Экстерн».
12. Подсистема обеспечения информационной безопасности Системы обеспечения безопасности информации Федерального казначейства
13. Единая система нормативной справочной информации
14. Платформа государственных сервисов
15. Государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»
16. Государственная автоматизированная информационная система «Управление»

17. Конструктор цифровых регламентов Федеральной государственной информационной системы «Федеральный реестр государственных и муниципальных услуг (функций)»

18. Федеральная государственная информационная система учета информационных систем (АИС Учета)

19. Федеральная государственная информационная система учета информационных систем (База знаний Центра ПРЦТ РАНХиГС)

20. Федеральная государственная информационная система координации информатизации

21. Информационная система «Генеральная схема развития сетей связи и инфраструктуры хранения и обработки данных Российской Федерации»

22. Координационный центр Правительства РФ

23. Информационная система «Инцидент Менеджмент»

24. Автоматизированная информационная система «Всероссийская система сбора и распределения контента по реализации нацпроектов в регионах»

25. Система «ОНФ.Помощь»

26. Государственная информационная система "Региональная геоинформационная система "Кузбасс"

27. Портал Систем электронных паспортов

Приложение № 13
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Перечень помещений Министерства цифрового развития и связи Кузбасса, в которых осуществляется обработка персональных данных

1. г. Кемерово, ул. Арочная 37а, каб. 315,
2. г. Кемерово, ул. Арочная 37а, каб. 408,412,413,414,
3. г. Кемерово, ул. Арочная 37а, каб. 501-507,512.

Приложение № 14
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Форма перечня лиц, допущенных в помещения, в которых производится обработка персональных данных

УТВЕРЖДАЮ
министр цифрового развития и связи Кузбасса
ФИО_____

«__» _____ 2022 г.

№ п/п	Фамилия Имя Отчество	Адрес и место расположения
1	Фамилия Имя Отчество	Название улицы, номер дома, номер кабинета/помещения
2	Фамилия Имя Отчество	
3	Фамилия Имя Отчество	
4	…	

Доступ в помещение посторонних лиц допускается только в сопровождении сотрудников из данного перечня.

Оборотная сторона перечня

Лист ознакомления с перечнем

№ п/п	Ф.И.О. работника	Должность работника	Дата ознакомления с перечнем	Личная подпись
1	Фамилия, инициалы			
2	…			
3	…			

Приложение № 15
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

ПОЛИТИКА
обеспечения безопасности персональных данных в информационных системах персональных данных Министерства цифрового развития и связи Кузбасса

Определения

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может

быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

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

доступ), обезличивание, блокирование, удаление, уничтожение информации (персональных данных).

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

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

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

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность

несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации (персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

Администратор ИБ	– администратор информационной безопасности
АРМ	– автоматизированное рабочее место
ЗИ	– защищаемая информация, в том числе, персональные данные, содержащаяся в базах данных
ИС	– информационная система
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПО	– программное обеспечение
СЗИ	– система защиты информации
СрЗИ	– средство защиты информации
ЭВМ	– электронно-вычислительная машина

1 Введение

1.1 Настоящая Политика в отношении обработки информации и персональных данных в ИС Министерства цифрового развития и связи Кузбасса (далее – Политика) определяет основные цели и задачи, а также общую стратегию построения СЗИ в ИС Министерства цифрового развития и связи Кузбасса. Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

1.2 Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности, который предполагает проведение комплекса мероприятий, включающих исследование угроз

информационной безопасности и разработку СЗИ, с позиции комплексного применения организационных, технических мер и СрЗИ.

1.3 Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности в ИС Министерства цифрового развития и связи Кузбасса, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации. Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности защищаемой информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз защищаемой информации;
- координации деятельности уполномоченных лиц при проведении работ по развитию и эксплуатации ИС Министерства цифрового развития и связи Кузбасса с соблюдением требований обеспечения безопасности защищаемой информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности защищаемой информации в ИС Министерства цифрового развития и связи Кузбасса.

1.4 Политика разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системах персональных данных»

1.5 В Политике определены требования к персоналу, работающему в ИС Министерства цифрового развития и связи Кузбасса, их степень ответственности и должностные обязанности, а также должностные обязанности сотрудников, ответственных за обеспечение безопасности защищаемой информации в ИС Министерства цифрового развития и связи Кузбасса.

2 Общие положения

2.1 Целью настоящей Политики является обеспечение безопасности защищаемой информации в ИС Министерства цифрового развития и связи Кузбасса от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации.

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

2.3 Защищаемая информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности защищаемой информации.

3 Область действия

3.1 Требования настоящей Политики распространяются на всех сотрудников, допущенных к работе в ИС Министерства цифрового развития и связи Кузбасса, а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4 Система защиты информации

4.1 СЗИ, строится на основании:

- Перечня обрабатываемой информации и персональных данных в ИС «Название организации»;
- Акта классификации ИС Министерства цифрового развития и связи Кузбасса;
- Акта определения уровня защищенности персональных данных, обрабатываемых в ИС Министерства цифрового развития и связи Кузбасса;
- Модели угроз и модели нарушителя безопасности информации, при ее обработке в ИС Министерства цифрового развития и связи Кузбасса (далее – Модель угроз);
- Технического задания на выполнение работ по развитию и обеспечению функционирования системы защиты персональных данных в ИС Министерства цифрового развития и связи Кузбасса;
- Руководящих документов ФСТЭК России и ФСБ России.

4.2 На основании этих документов определяется необходимый уровень защищенности информации, обрабатываемой в ИС Министерства цифрового развития и связи Кузбасса. На основании анализа актуальных угроз безопасности защищаемой информации, описанного в Отчете об обследовании и Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации.

4.3 В зависимости от уровня защищенности сегмента ИС и актуальных угроз, СЗИ может включать следующие подсистемы:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей персональных данных;

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и информации;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– управление конфигурацией информационной системы и системы защиты персональных данных.

4.4 В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки информации, операционными системами, прикладным программным обеспечением и специальными комплексами, реализующими СрЗИ.

5 Основные принципы построения СЗИ

5.1 Построение СЗИ сегмента ИС и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

5.2 Законность.

Данный принцип предполагает осуществление защитных мероприятий и разработку СЗИ в соответствии с действующим законодательством в

области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Сотрудники и обслуживающий персонал сегмента ИС должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

5.3 Системность.

Системный подход к построению СЗИ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации сегмента ИС. При создании СЗИ должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.4 Комплексность.

Комплексное использование методов и средств защиты информации предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

5.5 Непрерывность защиты информации.

Защита информации – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных СрЗИ, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла сегмента ИС. Сегмент ИС должен находиться в защищенном состоянии на протяжении всего времени своего функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты,

для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

5.6 Своевременность.

Данный принцип предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите сегмента ИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки в целом, и ее СЗИ, в частности. Разработка СЗИ должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

5.7 Преемственность и совершенствование.

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования сегмента ИС и его СЗИ с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.8 Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.9 Принцип минимизации полномочий.

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к защищаемой информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.10 Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность сегмента ИС, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за обеспечение безопасности информации и персональных данных и администратора ИБ.

5.11 Гибкость системы защиты информации.

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так

и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

5.12 Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

5.13 Научная обоснованность и техническая реализуемость.

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации. СЗИ должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.14 Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация СрЗИ должна осуществляться профессионально подготовленными специалистами.

5.15 Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

5.16 Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

6 Требования к подсистемам СЗИ

6.1 СЗИ включает в себя следующие организационные и технические меры защиты информации, реализуемые в информационных системах в рамках ее системы обеспечения информационной безопасности, в зависимости от угроз безопасности, используемых информационных технологий и структурно-функциональных характеристик автоматизированной системы:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей персональных данных;

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и информации;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– управление конфигурацией информационной системы и системы защиты персональных данных.

6.2 Подсистемы СЗИ имеют различный функционал в зависимости от уровня защищенности информации, обрабатываемой в ИС Министерства цифрового развития и связи Кузбасса.

6.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

6.2.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

6.2.3 Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или

исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

6.2.4 Меры по защите машинных носителей информации должны обеспечивать контроль доступа к машинным носителям информации и учет, контроль перемещения и использования.

6.2.5 Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6.2.6 Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

6.2.7 Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

6.2.8 Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

6.2.9 Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

6.2.10 Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

6.2.11 Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным

системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам.

6.2.12 Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

6.2.13 Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

6.2.14 Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечить управление изменениями конфигурации информационной системы, анализировать потенциальное воздействие планируемых изменений в конфигурации информационной системы и системы защиты персональных данных, а также определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.

7 Пользователи сегмента ИС

7.1 В ИС Министерства цифрового развития и связи Кузбасса можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой информации:

- администратор ИБ;
- ответственный за организацию обработки информации и персональных данных;
- ответственный пользователь криптосредств;
- пользователь.

7.2 Администратор ИБ

Администратор ИБ ответственен за функционирование СЗИ, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении сегмента ИС;
- обладает полной информацией о технических средствах и конфигурации сегмента ИС;

– имеет доступ ко всем техническим средствам обработки информации и данным сегмента ИС;

– обладает полной информацией о ИС Министерства цифрового развития и связи Кузбасса;

– имеет полный доступ к СрЗИ и протоколирования и к части ключевых элементов сегмента ИС.

Администратор ИБ уполномочен:

– реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов в соответствии с которыми пользователь получает возможность работать с элементами сегмента ИС;

– осуществлять аудит СрЗИ.

7.3 Ответственный за организацию обработки информации и персональных данных

Ответственный за организацию обработки информации и персональных данных обладает следующим уровнем доступа и знаний:

– знает законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности;

– знает порядок использования, обработки и хранения конфиденциальной информации, в том числе персональных данных.

Ответственный за организацию обработки информации и персональных данных уполномочен:

– осуществлять внутренний контроль соблюдения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;

– доводить до сведения сотрудников положения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;

– предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению информационной безопасности;

– организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

7.4 Ответственный пользователь криптосредств

Ответственный пользователь криптосредств ответственен за функционирование СКЗИ.

Ответственный пользователь криптосредств обладает следующим уровнем доступа и знаний:

– обладает полной информацией о системном и прикладном программном обеспечении сегмента ИС;

– имеет частичный доступ к СрЗИ и протоколирования и к части ключевых элементов сегмента ИС.

– имеет полный доступ к СКЗИ.

Ответственный пользователь криптосредств уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, позволяющие пользователю работать с элементами сегмента ИС;
- осуществлять аудит СКЗИ.

7.5 Пользователь сегмента ИС.

Пользователь сегмента ИС осуществляет обработку защищаемой информации. Обработка информации включает: возможность просмотра защищаемой информации, ручной ввод информации в систему сегмента ИС, формирование справок и отчетов по информации, полученной из сегмента ИС. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗИ.

Пользователь сегмента ИС обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;
- располагает конфиденциальными данными, к которым имеет доступ.

8 Требования к персоналу по обеспечению защиты информации

8.1 Все сотрудники, являющиеся пользователями сегмента ИС, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемой информации и соблюдению режима безопасности информации.

8.2 При вступлении в должность нового сотрудника, ответственный за обеспечение безопасности информации и персональных данных обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования сегмента ИС.

8.3 Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами сегмента ИС и СЗИ.

8.4 Сотрудники, имеющие доступ к сегменту ИС, должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации).

8.5 Сотрудники, имеющие доступ к сегменту ИС, должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

8.6 Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

8.7 Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе в ИС Министерства цифрового развития и связи Кузбасса, третьим лицам.

8.8 При работе с защищаемой информацией в ИС Министерства цифрового развития и связи Кузбасса сотрудники обязаны обеспечить отсутствие возможности просмотра защищаемой информации третьими лицами с мониторов АРМ или терминалов.

8.9 При завершении работы в ИС Министерства цифрового развития и связи Кузбасса сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

8.10 Сотрудники должны быть проинформированы об угрозах нарушения режима безопасности информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

8.11 Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы сегмента ИС, могущих повлечь за собой угрозы безопасности информации, а также о выявленных ими событиях, затрагивающих безопасность информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности информации.

9 Должностные обязанности пользователей сегмента ИС

Должностные обязанности пользователей сегмента ИС описаны в должностных регламентах. Порядок действий пользователей сегмента ИС по исполнению должностных обязанностей описывается в следующих документах:

- инструкция администратора ИБ;
- инструкция пользователя системы защиты информации;
- инструкция ответственного за организацию обработки информации и персональных данных;
- инструкция ответственного пользователя криптосредств.

10 Ответственность пользователей сегмента ИС

10.1 В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

10.2 Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил

эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

10.3 При нарушениях сотрудниками сегмента ИС правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение № 16
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Форма разъяснения
субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне, _____,
(фамилия, имя, отчество (при наличии))
разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным лицам Министерства цифрового развития и связи Кузбасса.

В соответствии со статьями 26 и 42 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных федерального государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30 мая 2005 г. № 609, статьями 65 и 86 Трудового кодекса Российской Федерации Министерством цифрового развития и связи Кузбасса определен перечень персональных данных, который субъект персональных данных обязан предоставить уполномоченным лицам Министерства цифрового развития и связи Кузбасса в связи с поступлением, прохождением и прекращением государственной гражданской службы Кемеровской области – Кузбасса (работы). Без представления субъектом персональных данных обязательных для заключения служебного контракта (трудового договора) сведений служебный контракт (трудовой договор) не может быть заключен.

_____ _____
(дата) (подпись)

Приложение № 17
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Форма обязательства
государственного гражданского служащего Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

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

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

В соответствии со статьей 7 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные, ставшие известными мне в связи с исполнением должностных обязанностей, без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных, о государственной гражданской службе и о противодействии коррупции.

Положения законодательства Российской Федерации, предусматривающие ответственность за нарушение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», мне разъяснены.

_____ _____
(дата) (подпись)

Приложение № 18
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. №135-п

Форма обязательства
лица, замещающего должность, не являющейся должностью государственной гражданской службы Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____
_____
_____,
(фамилия, имя, отчество (при наличии), должность)
обязуюсь прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового контракта.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные, ставшие известными мне в связи с исполнением должностных обязанностей, без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных, о государственной гражданской службе и о противодействии коррупции.

Положения законодательства Российской Федерации, предусматривающие ответственность за нарушение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», мне разъяснены.

_____ _____
(дата) (подпись)

Приложение № 19
к приказу Министерства
цифрового развития и связи
Кузбасса
«08» декабря 2022 г. № 135-п

Согласие на обработку персональных данных государственных гражданских служащих Кемеровской области – Кузбасса в Министерстве цифрового развития и связи Кузбасса, а также иных субъектов персональных данных

Я, _____
(фамилия, имя, отчество (при наличии))
зарегистрированный(ая) по адресу: _____
_____
паспорт серия _____ № _____, выдан _____
_____
_____

в соответствии с требованиями статьи 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О защите персональных данных», статьи 42 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», закона Кемеровской области - Кузбасса от 22.12.2022 N 159-ОЗ «О некоторых вопросах прохождения государственной гражданской службы Кемеровской области - Кузбасса», даю согласие уполномоченным должностным лицам Министерства цифрового развития и связи Кузбасса, зарегистрированного по адресу: г. Кемерово, пр-кт. Советский, 62, на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) моих персональных данных, в том числе:

1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и отчества (при наличии) в случае их изменения; сведения о том, когда, где и по какой причине они изменялись);

2) дата рождения (число, месяц и год рождения);

3) место рождения;

4) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи;

5) фотография;

6) сведения о гражданстве;

7) адрес и дата регистрации по месту жительства (места пребывания);

8) адрес фактического проживания (места нахождения);

9) сведения о семейном положении, о составе семьи;

10) реквизиты свидетельств государственной регистрации актов гражданского состояния и содержащиеся в них сведения;

11) сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании, ученая степень, ученое звание (дата присвоения, реквизиты диплома, аттестата);

12) сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке (повышении квалификации), квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения);

13) сведения о владении иностранными языками и языками народов Российской Федерации;

14) сведения о трудовой деятельности до поступления на государственную гражданскую службу (работу) в Министерство (подведомственные учреждения, находящиеся в ведении Министерства; территориальные органы федеральных служб, находящихся в ведении Министерства; организации, созданные для выполнения задач, поставленных перед Министерством);

15) сведения о классном чине федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное звание, классный чин правоохранительной службы, классный чин юстиции (кем и когда присвоены);

16) сведения о родителях, детях, сестрах, братьях, о супруге (бывшем или бывшей супруге) (дата рождения, место рождения, места работы (службы), домашний адрес);

17) сведения о форме и дате оформления допуска к государственной тайне,
ранее имевшемся и (или) имеющемся;

18) сведения о государственных наградах, иных наградах и знаках отличия;

19) сведения о пребывании за границей (когда, где, с какой целью);

20) сведения о близких родственниках (родителях, братьях, сестрах, детях), а также супругах, в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество (при его наличии), с какого времени проживают за границей);

21) реквизиты страхового свидетельства обязательного пенсионного страхования, содержащиеся в нем сведения;

22) идентификационный номер налогоплательщика;

23) реквизиты страхового медицинского полиса обязательного медицинского страхования, содержащиеся в нем сведения;

24) сведения о воинском учете, реквизиты документов воинского учета, а также сведения, содержащиеся в документах воинского учета;

25) сведения о наличии (отсутствии) судимости;

26) данные из ФНС России о том, что гражданин не является индивидуальным предпринимателем; учредителем (участником), руководителем юридического лица; об отсутствии сведений в реестре дисквалифицированных лиц;

27) сведения о своих доходах, расходах, об имуществе и обязательствах имущественного характера, а также сведения о доходах, расходах, об имуществе и обязательствах имущественного характера своих супруга (супруги) и несовершеннолетних детей;

28) сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых гражданин, претендующий на замещение должности гражданской службы, гражданский служащий размещали общедоступную информацию, а также данные, позволяющие их идентифицировать;

29) номера контактных телефонов (домашнего, служебного, мобильного);

30) сведения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, подтвержденные заключением медицинского учреждения;

31) сведения об инвалидности, сроке действия установленной инвалидности;

32) иные сведения, которые я пожелал(а) сообщить о себе.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на государственную гражданскую службу Кемеровской области - Кузбасса, ее прохождением и прекращением (служебных (трудовых) и непосредственно связанных с ними отношений), для реализации полномочий, возложенных законодательством Российской Федерации на Министерство цифрового развития и связи Кузбасса.

Персональные данные, а именно: фамилию, имя, отчество (при наличии) разрешаю использовать в качестве общедоступных в электронной почте и системе электронного документооборота Министерства цифрового развития и связи Кузбасса, на официальном сайте Министерства цифрового развития и связи Кузбасса, а также в иных случаях, предусмотренных

законодательством Российской Федерации об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления.

Персональные данные, а именно: дату рождения (число, месяц и год рождения) и фотографию **разрешаю / не разрешаю** (нужное подчеркнуть) использовать в качестве общедоступных для публикации на внутреннем информационном портале Министерства, а также в иных случаях, предусмотренных законодательством Российской Федерации об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления.

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока государственной гражданской службы (работы) в Министерстве цифрового развития и связи Кузбасса;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных Министерство цифрового развития и связи Кузбасса вправе продолжить обработку персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; 2010, № 31, ст. 4173; 2011, № 31, ст. 4701; 2013, № 14, ст. 1651; № 30, ст. 4038; № 51, ст. 6683; 2014, № 23, ст. 2927; № 30, ст. 4217; 2016, № 27, ст. 4164; 2017, № 27, ст. 3945; № 31, ст. 4772);

4) после увольнения с государственной гражданской службы (прекращения трудовых отношений) персональные данные хранятся в Министерстве цифрового развития и связи Кузбасса в течение срока хранения документов, предусмотренного действующим законодательством Российской Федерации в области архивного дела;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения функций, возложенных законодательством Российской Федерации на Министерство цифрового развития и связи Кузбасса.

Дата начала обработки персональных данных:

_____ _____

(дата) (подпись)

Настоящее согласие дано мною «___» _____ 20___ года

Подпись _____