



РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
ПО БРЯНСКОЙ ОБЛАСТИ

П Р И К А З

09.10.2020

№ 79

Брянск

**Об обеспечении безопасности персональных данных федеральных государственных
гражданских служащих и работников в Управлении Роскомнадзора по Брянской
области**

В соответствии с Федеральным законом от 27 июля 2006г. N152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006г. N149-ФЗ «Об информации, информатизации и защите информации, Федеральным законом от 27 июля 2004г. N79-ФЗ «О государственной гражданской службе Российской Федерации», Указом Президент Российской Федерации от 30 мая 2005г. N609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», Постановлением Правительства Российской Федерации от 1 ноября 2012г. N1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008г. N687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012г. N211 «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», Трудовым кодексом Российской Федерации, в целях контроля организации работ, связанных с получением, учетом, обработкой, накоплением и хранением документов, содержащих сведения, отнесенных к персональным данным, с использованием средств

8800

автоматизации и без использования таких средств и в связи с проведенными организационно-штатными мероприятиями, п р и к а з ы в а ю:

1. Утвердить следующие документы, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

- Положение об организации работы с персональными данными федерального государственного гражданского служащего и ведение его личного дела в Управлении Роскомнадзора по Брянской области (Приложение N1);

- Положение об обработке и защите персональных данных в Управлении Роскомнадзора по Брянской области (Приложение N2);

- Инструкцию администратора безопасности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Управлении Роскомнадзора по Брянской области (Приложение N3);

- Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства российской федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (Приложение N4);

- Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение N5);

- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами Управления Роскомнадзора по Брянской области (Приложение N6);

- Правила работы с обезличенными данными (Приложение N7);

- Перечень информационных систем персональных данных Управления Роскомнадзора по Брянской области (Приложение N8);

- Перечень персональных данных, обрабатываемых в Управлении Роскомнадзора по Брянской области в связи с реализацией служебных отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций (Приложение N9);

- Перечень должностей служащих Управления Роскомнадзора по Брянской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (Приложение N10);

- Перечень должностей служащих и работников Управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществления доступа к персональным данным (Приложение N11);

- Должностной регламент ответственного за организацию обработки персональных данных в Управлении Роскомнадзора по Брянской области (Приложение N12);

- Типовое обязательство служащего (работника) Управления Роскомнадзора по Брянской области, 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 (Приложение N13);

- Типовую форму согласия на обработку персональных данных служащих (работников) Управления Роскомнадзора по Брянской области, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение N14);

- Порядок доступа сотрудников Управления Роскомнадзора по Брянской области в помещения, в которых ведется обработка персональных данных (Приложение N15);

- Типовую форму листа ознакомления с локальными нормативными правовыми актами Управления Роскомнадзора по Брянской области, направленными на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» (Приложение N16);

- Места хранения персональных данных (Приложение N17);

- Список должностных лиц имеющих доступ к персональным данным и личным делам государственных гражданских служащих и работников Управления (Приложение N18);

2. Назначить ответственным за организацию обработки персональных данных Управления – заместителя руководителя – начальника отдела Морозова Е.Е.;

3. Назначить администратором безопасности обработки персональных данных за обработку персон данных в информационных системах персональных данных ЕИС УКС и «1С: Предприятие» – начальника отдела организационной, финансовой, правовой работы и кадров Бирюлина З.В.;

4. Назначить ответственным за обеспечение безопасности обработки персональных данных в информационной системе «1С: Предприятие» – заместителя начальника отдела - главного бухгалтера Калиновскую О.М., за обеспечение безопасности обработки персональных данных гражданских служащих в ЕИС УКС и за обеспечение безопасности обработки персональных данных, содержащихся в личных делах – ведущий специалист-эксперт Шкурко М.И.

5. Приказы от 11.01.2009г. N2, от 06.01.2012г. N6, от 27.03.2012г. N40, 26.03.2013г. N31, от 28.10.2013г. N117, от 06.07.2015г. N65, от 17.10.2016г. N74, от 05.04.2019г. N20 считать утратившими силу.

6. Довести настоящий приказ до сведения всех сотрудников Управления.

7. Документы, связанные с политикой обработки персональных данных в Управлении Роскомнадзора по Брянской области разместить на странице сайта Управления в сети интернет. Ответственным за размещение информации назначить заместителя руководителя – начальника отдела – Морозова Е.Е.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель



Кузин Д.В.

ПРОЕКТ ПРИКАЗА ПОДГОТОВЛЕН:

Ведущий специалист – эксперт



М.И. Шкурко

**Положение об организации работы с персональными данными
федерального государственного гражданского служащего и ведение его
личного дела в Управлении Роскомнадзора по Брянской области**

1. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных федерального государственного гражданского служащего Управления Роскомнадзора по Брянской области (далее - гражданский служащий), а также ведения его личного дела в соответствии со статьей 42 Федерального закона «О государственной гражданской службе Российской Федерации».

2. Под персональными данными гражданского служащего понимаются сведения о фактах, событиях и обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность и содержащиеся в личном деле гражданского служащего либо подлежащие включению в его личное дело в соответствии с настоящим Положением.

3. Руководитель Управления Роскомнадзора по Брянской области (далее - Управление), осуществляющий полномочия нанимателя от имени Российской Федерации, и иные уполномоченные им лица, обеспечивают защиту персональных данных гражданских служащих, содержащихся в их личных делах, от неправомерного их использования или утраты.

4. Руководитель Управления определяет лиц, как правило, из числа работников ответственных за прохождение государственной службы и кадров, уполномоченных на обработку персональных данных государственных служащих (далее операторы), обеспечивающих обработку персональных данных в соответствии с требованиями Федеральных законов «О государственной гражданской службе Российской Федерации» и «О персональных данных», других нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

5. При обработке персональных данных гражданского служащего операторы обязаны соблюдать следующие требования:

а) обработка персональных данных гражданского служащего осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия гражданскому служащему в прохождении государственной гражданской службы Российской Федерации (далее - гражданская служба), в обучении и должностном росте, обеспечения личной безопасности гражданского служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества Управления, учета результатов исполнения им должностных обязанностей;

б) персональные данные следует получать лично у гражданского служащего. В случае возникновения необходимости получения персональных данных гражданского служащего у третьей стороны следует известить об этом гражданского служащего заранее, получить его письменное согласие и сообщить гражданскому служащему о целях, предполагаемых источниках и способах получения персональных данных;

в) запрещается получать, обрабатывать и приобщать к личному делу гражданского служащего не установленные Федеральными законами «О государственной

гражданской службе Российской Федерации» и «О персональных данных» персональные данные о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе профессиональных союзах;

г) при принятии решений, затрагивающих интересы гражданского служащего, запрещается основываться на персональных данных гражданского служащего полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

д) защита персональных данных гражданского служащего от неправомерного их использования или утраты обеспечивается за счет средств Управления Роскомнадзора в порядке, установленном Федеральными законами «О государственной гражданской службе Российской Федерации», «О персональных данных», Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации;

е) передача персональных данных гражданского служащего третьей стороне не допускается без письменного согласия гражданского служащего, за исключением случаев, установленных федеральными законами;

ж) обеспечение конфиденциальности персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

з) в случае выявления недостоверных персональных данных гражданского служащего или неправомерных действий с ними оператора при обращении или по запросу гражданского служащего, являющегося субъектом персональных данных, или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему гражданскому служащему, с момента такого обращения или получения такого запроса на период проверки;

и) в случае подтверждения факта недостоверности персональных данных гражданского служащего оператор на основании документов, представленных гражданским служащим, являющимся субъектом персональных данных, или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;

к) в случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения.

В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты неправомерности действий с персональными данными, обязан уточнить персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить гражданского служащего, являющегося субъектом персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;

л) хранение персональных данных должно осуществляться в форме, позволяющей определить гражданского служащего, являющегося субъектом персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

6. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме гражданского служащего, являющегося субъектом персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации о государственной службе, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию и другими нормативными правовыми актами Российской Федерации.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного и случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

7. Трансграничная передача персональных данных на территории иностранных государств осуществляется в соответствии с Федеральным законом «О персональных данных».

8. В целях обеспечения защиты персональных данных, хранящихся в личных делах гражданских служащих, гражданские служащие имеют право:

а) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные гражданского служащего, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

в) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона «О государственной гражданской службе Российской Федерации».

Гражданский служащий при отказе оператора исключить или исправить его персональные данные имеет право заявить в письменной форме руководителю Управления о своем несогласии, обосновав соответствующим образом такое несогласие.

Персональные данные оценочного характера гражданский служащий имеет право дополнить заявлением, выражающим его собственную точку зрения.

г) требовать от руководителя Управления уведомления всех лиц, которым ранее были сообщены неверные или неполные их персональные данные, обо всех произведенных в них изменениях или исключениях из них;

д) обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если гражданский служащий, являющийся субъектом персональных данных, считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы.

9. Гражданский служащий, виновный в нарушении норм, регулирующих получение, обработку, хранение и передачу персональных данных другого гражданского служащего, несет ответственность в соответствии с Федеральным законом «О государственной гражданской службе Российской Федерации» и другими федеральными законами.

10. В соответствии со статьей 15 Федерального закона от 27 мая 2003г. N 58-ФЗ «О системе государственной службы Российской Федерации» на основании персональных данных гражданских служащих в Управлении формируются и ведутся, в том числе на электронных носителях, реестры гражданских служащих.

11. Управление вправе подвергать обработке (в том числе автоматизированной) персональные данные гражданских служащих при формировании кадрового резерва.

12. В личное дело гражданского служащего вносятся его персональные данные и иные сведения, связанные с поступлением на гражданскую службу, ее прохождением и увольнением с гражданской службы и необходимые для обеспечения деятельности Управления.

Личное дело гражданского служащего ведется Управлением.

13. Персональные данные, внесенные в личные дела гражданских служащих, иные сведения, содержащиеся в личных делах гражданских служащих, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах

массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

14. К личному делу гражданского служащего приобщаются:

а) письменное заявление с просьбой о поступлении на гражданскую службу и замещении должности государственной гражданской службы Российской Федерации (далее - должность гражданской службы);

б) собственноручно заполненная и подписанная гражданином Российской Федерации анкета установленной формы с приложением фотографии;

в) документы о прохождении конкурса на замещение вакантной должности гражданской службы (если гражданин назначен на должность по результатам конкурса);

г) копия паспорта и копии свидетельств о государственной регистрации актов гражданского состояния;

д) копия трудовой книжки или документа, подтверждающего прохождение военной или иной службы;

е) копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

ж) копии решений о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премии (если таковые имеются);

з) копия акта государственного органа о назначении на должность гражданской службы;

и) экземпляр служебного контракта, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт,

к) копии актов государственного органа о переводе гражданского служащего на иную должность гражданской службы, о временном замещении им иной должности гражданской службы;

л) копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

м) копия акта государственного органа об освобождении гражданского служащего от замещаемой должности гражданской службы, о прекращении служебного контракта или его приостановлении;

н) аттестационный лист гражданского служащего, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

о) экзаменационный лист гражданского служащего и отзыв об уровне его знаний, навыков и умений (профессиональном уровне) и о возможности присвоения ему классного чина государственной гражданской службы Российской Федерации;

п) копии документов о присвоении гражданскому служащему классного чина государственной гражданской службы Российской Федерации (иного класса чина, квалификационного разряда, дипломатического ранга);

р) копии документов о включении гражданского служащего в кадровый резерв, а также об исключении его из кадрового резерва;

с) копии решений о поощрении гражданского служащего, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

т) копии документов о начале служебной проверки, ее результатах, отстранении гражданского служащего от замещаемой должности гражданской службы;

у) документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности гражданской службы связано с использованием таких сведений;

ф) сведения о доходах, имуществе и обязательствах имущественного характера гражданского служащего;

- х) копия страхового свидетельства обязательного пенсионного страхования;
- ц) копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;
- ч) копия страхового медицинского полиса обязательного медицинского страхования граждан;
- ш) медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению;

щ) справка о результатах проверки достоверности и полноты, представленных гражданским служащим сведений о доходах, имуществе и обязательствах имущественного характера, а также сведений о соблюдении гражданским служащим ограничений, установленных федеральными законами.

15. В личное дело гражданского служащего вносятся также письменные объяснения гражданского служащего, если такие объяснения даны им после ознакомления с документами своего личного дела.

К личному делу гражданского служащего приобщаются иные документы, предусмотренные федеральными законами и иными нормативными правовыми актами Российской Федерации.

16. Документы, приобщенные к личному делу гражданского служащего, брошюруются, страницы нумеруются, к личному делу прилагается опись.

Учетные данные гражданских служащих в соответствии с порядком, установленным Президентом Российской Федерации, хранятся Управлением Роскомнадзора на электронных носителях. Управление Роскомнадзора обеспечивает их защиту от несанкционированного доступа и копирования.

17. В обязанности Управления, осуществляющего ведение личных дел гражданских служащих, входит:

- а) приобщение документов, указанных в пунктах 14 и 15 настоящего Положения, к личным делам гражданских служащих;
- б) обеспечение сохранности личных дел гражданских служащих;
- в) обеспечение конфиденциальности сведений, содержащихся в личных делах гражданских служащих, в соответствии с Федеральным законом «О государственной гражданской службе Российской Федерации», другими федеральными законами, иными нормативными правовыми актами Российской Федерации, а также в соответствии с настоящим Положением;
- г) ознакомление гражданского служащего с документами своего личного дела не реже одного раза в год, а также по просьбе гражданского служащего и во всех иных случаях, предусмотренных законодательством Российской Федерации.

18. Гражданские служащие, уполномоченные на ведение и хранение личных дел гражданских служащих, могут привлекаться в соответствии с законодательством Российской Федерации к дисциплинарной и иной ответственности за разглашение конфиденциальных сведений, содержащихся в указанных личных делах, а также за иные нарушения порядка ведения личных дел гражданских служащих, установленного настоящим Положением.

19. При переводе гражданского служащего на должность гражданской службы в другом государственном органе его личное дело передается в государственный орган по новому месту замещения должности гражданской службы.

20. При назначении гражданского служащего на государственную должность Российской Федерации или государственную должность субъекта Российской Федерации его личное дело передается в государственный орган по месту замещения государственной должности Российской Федерации или государственной должности субъекта Российской Федерации.

21. Личные дела гражданских служащих, уволенных с гражданской службы (за исключением гражданских служащих, указанных в пункте 20 настоящего Положения),

хранятся Управлением в течение 10 лет со дня увольнения с гражданской службы, после чего передаются в архив.

Если гражданин, личное дело которого хранится Управлением, поступит на гражданскую службу вновь, его личное дело подлежит передаче Управлением в государственный орган по месту замещения должности гражданской службы.

Личные дела гражданских служащих, содержащие сведения, составляющие государственную тайну, хранятся Управлением в соответствии с законодательством Российской Федерации о государственной тайне.

Положение
об обработке и защите персональных данных в Управлении
Роскомнадзора по Брянской области

I. Общие положения

1.1. Положение об обработке и защите персональных данных в Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Брянской области (далее - Положение) определяет 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 Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Брянской области (далее - Управление).

1.2. Настоящее Положение определяет политику Управления как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации (Собрание законодательства Российской Федерации, 2002, N 1, ст. 3; N 30, ст. 3014, 3033; 2003, N 27, ст. 2700; 2004, N 18, ст. 1690; N 35, ст. 3607; 2005, N 1, ст. 27; N 19, ст. 1752; 2006, N 27, ст. 2878; N 52, ст. 5498; 2007, N 1, ст. 34; N 17, ст. 1930; N 30, ст. 3808; N 41, ст. 4844; N 43, ст. 5084; N 49, ст. 6070; 2008, N 9, ст. 812; N 30, ст. 3613; N 30, ст. 3616; N 52, ст. 6235, 6236; 2009, N 1, ст. 17, 21; N 19, ст. 2270; N 29, ст. 3604; N 30, ст. 3732, 3739; N 46, ст. 5419; N 48, ст. 5717; 2010, N 31, ст. 4196; N 52, ст. 7002; 2011, N 1, ст. 49; N 25, ст. 3539; N 27, ст. 3880; N 30, ст. 4586, 4590, 4591, 4596; N 45, ст. 6333, 6335; N 48, ст. 6730, 6735; N 49, ст. 7031; 2012, N 10, ст. 1164; N 14, ст. 1553; N 18, ст. 2127; N 31, ст. 4325) (далее - Трудовой кодекс Российской Федерации), Кодексом Российской Федерации об административных правонарушениях (Собрание законодательства Российской Федерации, 2002, N 1, ст. 1; N 18, ст. 1721; N 30, ст. 3029; N 44, ст. 4295, 4298; 2003, N 27, ст. 2700, 2708, 2717; N 46, ст. 4434, 4440; N 50, ст. 4847, 4855; N 52, ст. 5037; 2004, N 19, ст. 1838; N 30, ст. 3095; N 31, ст. 3229; N 34, ст. 3529, 3533; N 44, ст. 4266; 2005, N 1, ст. 9, 13, 37, 40, 45; N 10, ст. 762, 763; N 13, ст. 1077, 1079; N 17, ст. 1484; N 19, ст. 1752; N 25, ст. 2431; N 27, ст. 2719, 2721; N 30, ст. 3104; N 30, ст. 3124, 3131; N 40, ст. 3986; N 50, ст. 5247; N 52, ст. 5574, 5596; 2006, N 1, ст. 4, 10; N 2, ст. 172, 175; N 6, ст. 636; N 10, ст. 1067; N 12, ст. 1234; N 17, ст. 1776; N 18, ст. 1907; N 19, ст. 2066; N 23, ст. 2380, 2385; N 28, ст. 2975; N 30, ст. 3287; N 31, ст. 3420, 3432, 3433, 3438, 3452; N 43, ст. 4412; N 45, ст. 4633, 4634, 4641; N 50, ст. 5279, 5281; N 52, ст. 5498; 2007, N 1, ст. 21, 25, 29, 33; N 7, ст. 840; N 15, ст. 1743; N 16, ст. 1824, 1825; N 17, ст. 1930; N 20, ст. 2367; N 21, ст. 2456; N 26, ст. 3089; N 30, ст. 3755; N 31, ст. 4001, 4007, 4008, 4009, 4015; N 41, ст. 4845; N 43, ст. 5084; N 46, ст. 5553; N 49, ст. 6034, 6065; N 50, ст. 6246; 2008, N 10, ст. 896; N 18, ст. 1941; N 20, ст. 2251, 2259; N 29, ст. 3418; N 30, ст. 3582, 3601, 3604; N 45, ст. 5143; N 49, ст. 5738, 5745, 5748; N 52, ст. 6227, 6235, 6236, 6248; 2009, N 1, ст. 17; N 7, ст. 771, 777; N 19, ст. 2276; N 23, ст. 2759, 2767, 2776; N 26, ст. 3120, 3122, 3131, 3132; N 29, ст. 3597, 3599, 3635, 3642; N 30, ст. 3735, 3739; N 45, ст. 5265, 5267; N 48, ст. 5711, 5724, 5755; 2010, N 1, ст. 1; N 11, ст. 1169, 1176; N 15, ст. 1743, 1751; N 18, ст. 2145; N 19, ст. 2291; N 21, ст. 2524, 2525, 2526, 2530; N 23, ст. 2790; N 25, ст. 3070; N 27, ст. 3416, 3429; N 28, ст. 3553; N 30, ст. 4000, 4002, 4005, 4006, 4007; N 31, ст. 4155, 4158,

4164, 4191, 4192, 4193, 4195, 4198, 4206, 4207, 4208; N 32, ст. 4298; N 41, ст. 5192, 5193; N 46, ст. 5918; N 49, ст. 6409; N 50, ст. 6605; N 52, ст. 6984, 6995, 6996; 2011, N 1, ст. 10, 23, 29, 33, 47, 54; N 7, ст. 901; N 15, ст. 2039, 2041; N 17, ст. 2310, 2312; N 19, ст. 2714, 2715; N 23, ст. 3260, 3267; N 27, ст. 3873, 3881; N 29, ст. 4289, 4290, 4291, 4298; N 30, ст. 4573, 4574, 4584, 4585, 4590, 4591, 4598, 4600, 4601, 4605; N 45, ст. 6325, 6326, 6334; N 46, ст. 6406; N 47, ст. 6601, 6602; N 48, ст. 6730, 6732; N 49, ст. 7025, 7042, 7056, 7061; N 50, ст. 7342, 7345, 7346, 7351, 7352, 7355, 7362, 7366; 2012, N 6, ст. 621; N 10, ст. 1166; N 15, ст. 1723, ст. 1724; N 18, ст. 2126, ст. 2128; N 19, ст. 2278; N 24, ст. 3068, ст. 3069, ст. 3082; N 29, ст. 3996; N 31, ст. 4320, ст. 4322, ст. 4330; N 41, ст. 5523), Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; N 52, ст. 6974; 2011, N 23, ст. 3263; N 31, ст. 4701) (далее - Федеральный закон "О персональных данных"), Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328), Федеральным законом от 27 мая 2003 г. N 58-ФЗ "О системе государственной службы Российской Федерации" (Собрание законодательства Российской Федерации, 2003, N 22, ст. 2063; N 46, ст. 4437; 2006, N 29, ст. 3123; 2007, N 49, ст. 6070; 2011, N 1, ст. 31; N 50, ст. 7337) (далее - Федеральный закон "О системе государственной службы Российской Федерации"), Федеральным законом от 27 июля 2004 г. N 79-ФЗ "О государственной гражданской службе Российской Федерации" (Собрание законодательства Российской Федерации, 2004, N 31, ст. 3215; 2006, N 6, ст. 636; 2007, N 10, ст. 1151; N 16, ст. 1828; N 49, ст. 6070; 2008, N 13, ст. 1186; N 30, ст. 3616; N 52, ст. 6235; 2009, N 29, ст. 3597, 3624; N 48, ст. 5719; N 51, ст. 6150, 6159; 2010, N 5, ст. 459; N 7, ст. 704; 2011, N 1, ст. 31; N 27, ст. 3866; N 29, ст. 4295; N 48, ст. 6730; N 50, ст. 7337) (далее - Федеральный закон "О государственной гражданской службе Российской Федерации"), Федеральным законом от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции" (Собрание законодательства Российской Федерации, 2008, N 52, ст. 6228; 2011, N 29, ст. 4291; N 48, ст. 6730) (далее - Федеральный закон "О противодействии коррупции"), Федеральным законом от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" (Собрание законодательства Российской Федерации, 2010, N 31, ст. 4179; 2011, N 15, ст. 2038; N 27, ст. 3880; N 29, ст. 4291; N 30, ст. 4587; N 49, ст. 7061; 2012, N 31, ст. 4322) (далее - Федеральный закон "Об организации предоставления государственных и муниципальных услуг"), Федеральным законом от 2 сентября 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" (Собрание законодательства Российской Федерации, 2006, N 19, ст. 2060; 2010, N 27, ст. 3410; N 31, ст. 4196) (далее - Федеральный закон "О порядке рассмотрения обращений граждан Российской Федерации"), Федеральным законом от 7 июля 2003 г. N 126-ФЗ "О связи" (Собрание законодательства Российской Федерации, 2003, N 28, ст. 2895; N 52, ст. 5038; 2004, N 35, ст. 3607; N 45, ст. 4377; 2005, N 19, ст. 1752; 2006, N 6, ст. 636; N 10, ст. 1069; N 31, ст. 3431, ст. 3452; 2007, N 1, ст. 8; N 7, ст. 835; 2008, N 18, ст. 1941; 2009, N 29, ст. 3625; 2010, N 7, ст. 705; N 15, ст. 1737; N 27, ст. 3408; N 31, ст. 4190; 2011, N 7, ст. 901; N 9, ст. 1205; N 25, ст. 3535; N 27, ст. 3873, ст. 3880; N 29, ст. 4284, ст. 4291; N 30, ст. 4590; N 45, ст. 6333; N 49, ст. 7061; N 50, ст. 7351, ст. 7366; 2012, N 31, ст. 4328), Федеральным законом от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322) (далее - Федеральный закон "О лицензировании отдельных видов деятельности"), Законом Российской Федерации от 27 декабря 1991 г. N 2124-1 "О средствах массовой информации" (Российская газета, 1992, 8 февраля, N 32; Собрание законодательства Российской Федерации, 1995, N 3, ст. 169; N 24, ст. 2256; N 30, ст. 2870; 1996, N 1, ст. 4; 1998, N 10, ст. 1143; 2000, N 26, ст. 2737; N 32, ст. 3333; 2001, N 32, ст. 3315; 2002, N 12, ст. 1093; N 30, ст. 3029, ст. 3033; 2003, N 27, ст.

2708; N 50, ст. 4855; 2004, N 27, ст. 2711; N 35, ст. 3607; N 45, ст. 4377; 2005, N 30, ст. 3104; N 31, ст. 3452; 2006, N 43, ст. 4412; 2007, N 31, ст. 4008; 2008, N 52, ст. 6236; 2009, N 7, ст. 778; 2011, N 25, ст. 3535; N 29, ст. 4291; 2012, N 31, ст. 4322) (далее - Закон Российской Федерации "О средствах массовой информации"), Указом Президента Российской Федерации от 1 февраля 2005 г. N 112 "Об утверждении Положения о конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации" (Собрание законодательства Российской Федерации, 2005, N 6, ст. 439; 2011, N 4, ст. 578), Указом Президента Российской Федерации от 30 мая 2005 г. N 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела" (Собрание законодательства Российской Федерации, 2005, N 23, ст. 2242; 2008, N 43, ст. 4921), постановлением Правительства Российской Федерации от 16 марта 2009 г. N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (Собрание законодательства Российской Федерации, 2009, N 12, ст. 1431; 2010, N 13, ст. 1502; N 26, ст. 3350; 2011, N 3, ст. 542; N 6, ст. 888; N 14, ст. 1935; N 21, ст. 2965; N 40, ст. 5548; N 44, ст. 6272; 2012, N 20, ст. 2540; N 39, ст. 5270), постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257), постановлением Правительства Российской Федерации от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" (Собрание законодательства Российской Федерации, 2008, N 28, ст. 3384), постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" (Собрание законодательства Российской Федерации, 2008, N 38, ст. 4320), постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" (Собрание законодательства Российской Федерации, 2012, N 14, ст. 1626), постановлением Правительства Российской Федерации от 10 сентября 2009 г. N 723 "О порядке ввода в эксплуатацию отделанных государственных информационных систем" (Собрание законодательства Российской Федерации, 2009, N 37, ст. 4416; 2012, N 27, ст. 3753), постановлением Правительства Российской Федерации от 27 января 2009 г. N 63 "О предоставлении федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения" (Собрание законодательства Российской Федерации, 2009, N 6, ст. 739; N 51, ст. 6328; 2010, N 9, ст. 963; N 52, ст. 7104) (далее - постановление Правительства Российской Федерации "О предоставлении федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения"), распоряжением Правительства Российской Федерации от 26 мая 2005 г. N 667-р об утверждении формы анкеты, подлежащей представлению в государственный орган гражданином Российской Федерации, изъявившим желание участвовать в конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации (Собрание законодательства Российской Федерации, 2005, N 22, ст. 2192; 2007, N 43, ст. 5264), распоряжением Правительства Российской Федерации от 6 октября 2011 г. N 1752-р об утверждении перечня документов, прилагаемых заявителем к заявлению о регистрации (перерегистрации) средства массовой информации (Собрание законодательства Российской Федерации, 2011, N 41, ст. 5789), приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"

(зарегистрирован Министерством юстиции Российской Федерации 3 апреля 2008 г., регистрационный N 11462).

1.4. Обработка персональных данных в Управлении осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

II. Условия и порядок обработки персональных данных государственных гражданских служащих и работников Управления Роскомнадзора по Брянской области

2.1. Персональные данные государственных гражданских служащих Управления, граждан, претендующих на замещение должностей государственной гражданской службы Управления обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия государственным служащим Управления в прохождении государственной службы, формирования кадрового резерва государственной гражданской службы, обучения и должностного роста, учета результатов исполнения государственными служащими Управления должностных обязанностей, обеспечения личной безопасности государственных служащих Управления и членов их семьи, обеспечения государственным служащим Управления установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

2.2. В целях, указанных в пункте 2.1 настоящего Положения, обрабатываются следующие категории персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления Роскомнадзора по Брянской области:

2.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2.2.2. число, месяц, год рождения;

2.2.3. место рождения;

2.2.4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

2.2.5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

2.2.6. адрес места жительства (адрес регистрации, фактического проживания);

2.2.7. номер контактного телефона или сведения о других способах связи;

2.2.8. реквизиты страхового свидетельства государственного пенсионного страхования;

2.2.9. идентификационный номер налогоплательщика;

2.2.10. реквизиты страхового медицинского полиса обязательного медицинского страхования;

2.2.11. реквизиты свидетельства государственной регистрации актов гражданского состояния;

2.2.12. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

2.2.13. сведения о трудовой деятельности;

2.2.14. сведения о воинском учете и реквизиты документов воинского учета;

2.2.15. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

2.2.16. сведения об ученой степени;

2.2.17. информация о владении иностранными языками, степень владения;

2.2.18. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

2.2.19. фотография;

2.2.20. сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы;

2.2.21. информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту;

2.2.22. сведения о пребывании за границей;

2.2.23. информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

2.2.24. информация о наличии или отсутствии судимости;

2.2.25. информация об оформленных допусках к государственной тайне;

2.2.26. государственные награды, иные награды и знаки отличия;

2.2.27. сведения о профессиональной переподготовке и (или) повышении квалификации;

2.2.28. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

2.2.29. ¹ сведения о доходах, об имуществе и обязательствах имущественного характера;

2.2.30. номер расчетного счета;

2.2.31. номер банковской карты;

2.2.32. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1 настоящего Положения.

2.3. Обработка персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.1 настоящего Положения, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона "О персональных данных" и положениями Федерального закона "О

системе государственной службы Российской Федерации", Федерального закона "О государственной гражданской службе Российской Федерации", Федерального закона "О противодействии коррупции", Трудовым кодексом Российской Федерации.

2.4. Обработка специальных категорий персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.1 настоящего Положения, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона "О персональных данных" и положениями Трудового кодекса Российской Федерации, за исключением случаев получения персональных данных работника у третьей стороны (в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие сотрудников и граждан, претендующих на замещение указанной должности).

2.5. Обработка персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы осуществляется при условии получения согласия указанных лиц в следующих случаях:

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

2.5.2. при трансграничной передаче персональных данных;

2.5.3. 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.

2.6. В случаях, предусмотренных пунктом 2.5 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом "О персональных данных".

2.7. Обработка персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы осуществляется специалистом отдела организационной, финансовой, правовой работы и кадров, ответственным за организацию кадровой работы Управления и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы осуществляется путем:

2.8.1. получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в кадровое подразделение Управления);

2.8.2. копирования оригиналов документов;

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

2.8.4. формирования персональных данных в ходе кадровой работы;

2.8.5. внесения персональных данных в информационные системы Управления, используемые отделом, ответственным за кадровую работу.

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных

непосредственно от государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы.

2.10. В случае возникновения необходимости получения персональных данных государственного служащего Управления у третьей стороны, следует известить об этом государственного служащего заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

2.11. Запрещается получать, обрабатывать и приобщать к личному делу государственного служащего Управления персональные данные, не предусмотренные пунктом 2.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.12. При сборе персональных данных сотрудник, отвечающий за кадровую работу в Управлении, осуществляющий сбор (получение) персональных данных непосредственно от государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.13. Передача (распространение, предоставление) и использование персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

III. Условия и порядок обработки персональных данных государственных служащих Управления и лиц, состоящих с ними в родстве (свойстве), в связи с рассмотрением вопроса о предоставлении единовременной субсидии на приобретение жилого помещения

3.1. В Управлении осуществляется обработка персональных данных государственных служащих, состоящих с ними в родстве (свойстве), в связи с рассмотрением вопроса о предоставлении единовременной субсидии на приобретение жилого помещения.

3.2. Перечень персональных данных, подлежащих обработке в связи с предоставлением единовременной субсидии на приобретение жилого помещения, определяется постановлением Правительства Российской Федерации "О предоставлении федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения", и включает в себя:

3.2.1. фамилию, имя, отчество;

3.2.2. вид, серию, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дату выдачи;

3.2.3. адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);

3.2.4. сведения о составе семьи;

3.2.5. 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 государственного служащего 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;

3.2.6. иные персональные данные, предусмотренные законодательством Российской Федерации.

3.3. Обработка персональных данных государственных служащих Управления при постановке на учет для получения единовременной выплаты осуществляется на основании заявления государственного служащего, представляемого на имя руководителя Роскомнадзора в Комиссию Роскомнадзора по рассмотрению вопросов о постановке на учет федеральных государственных гражданских служащих для получения единовременной субсидии на приобретение жилого помещения (далее - Комиссия Роскомнадзора).

3.4. Обработка персональных данных государственных служащих Управления в связи с предоставлением единовременной субсидии на приобретение жилого помещения, в частности сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных, осуществляется должностными лицами Управления, входящими в состав Комиссии, путем:

3.4.1. получения оригиналов необходимых документов;

3.4.2. предоставления заверенных в установленном порядке копий документов.

3.5. Комиссия Роскомнадзора вправе проверять сведения, содержащиеся в документах, представленных государственными служащими о наличии условий, необходимых для постановки государственного служащего на учет для получения единовременной субсидии на получение жилья.

3.6. Передача (распространение, предоставление) и использование персональных данных государственных служащих Управления, полученных в связи с предоставлением единовременной субсидии на приобретение жилого помещения, осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

IV. Условия и порядок обработки персональных данных субъектов в связи с предоставлением государственных услуг и исполнением государственных функций

4.1. В Управлении Роскомнадзора по Брянской области обработка персональных данных физических лиц осуществляется в целях предоставления следующих государственных услуг и исполнения государственных функций:

4.1.1. организация приема граждан, обеспечение своевременного и в полном объеме рассмотрения устных и письменных обращений граждан по вопросам, относящимся к компетенции Управления Роскомнадзора по Брянской области;

4.1.2. регистрация средств массовой информации;

4.1.3. разрешительная деятельность в области связи;

4.1.4. ведение реестра операторов осуществляющих обработку персональных данных

4.1.5. мероприятия по привлечению к административной ответственности.

4.2. Персональные данные граждан, обратившихся в Управление Роскомнадзора по Брянской области лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в Управлении Роскомнадзора по Брянской области подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

4.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

4.3.1. фамилия, имя, отчество (последнее при наличии);

4.3.2. почтовый адрес;

4.3.3. адрес электронной почты;

4.3.4. указанный в обращении контактный телефон;

4.3.5. наличие второго гражданства;

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

4.4. При регистрации средств массовой информации осуществляется обработка следующих персональных данных заявителей:

4.4.1. фамилия, имя, отчество (последнее при наличии);

4.4.2. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

4.4.3. адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);

4.4.4. номер контактного телефона или сведения о других способах связи;

4.4.5. наличие второго гражданства.

4.5. В рамках разрешительной деятельности в области связи могут обрабатываться следующие персональные данные заявителей:

4.5.1. фамилия, имя, отчество (последнее при наличии);

4.5.2. вид, серия, номер документа, удостоверяющего личность;

4.5.3. адрес места жительства;

4.5.4. номер контактного телефона и, при наличии, адрес электронной почты;

4.5.5. наличие второго гражданства;

4.6. При ведении реестра операторов осуществляющих обработку персональных данных осуществляется обработка следующих персональных данных:

4.6.1. ИНН;

4.6.2. фамилия, имя, отчество (последнее при наличии);

4.6.3. адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);

4.6.4. номер контактного телефона или сведения о других способах связи;

4.6.5. ОГРНИП;

4.6.6. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

4.6.7. наличие второго гражданства.

4.7. При проведении мероприятий по привлечению к административной ответственности подлежат обработке следующие персональные данные:

4.7.1. фамилия, имя, отчество (последнее при наличии);

4.7.2. адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);

4.7.3. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

4.7.4. номер контактного телефона или сведения о других способах связи;

4.7.5. наличие второго гражданства.

4.8. В рамках осуществления деятельности по защите прав субъектов персональных данных осуществляется обработка следующих персональных данных заявителей:

4.8.1. фамилия, имя, отчество (последнее при наличии);

4.8.2. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

4.8.3. почтовый адрес места жительства;

4.8.4. адрес электронной почты;

4.8.5. номер телефона;

4.8.6. идентификационный номер налогоплательщика;

4.8.7. сведения о трудовой деятельности и реквизиты трудовой книжки;

4.8.8. наличие второго гражданства;

4.8.9. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

4.9. Обработка персональных данных, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, указанных в пункте 4.1 настоящего Положения, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона "О персональных данных", Федеральными законами "Об организации предоставления государственных и муниципальных услуг", "О порядке рассмотрения обращений граждан Российской Федерации", "О лицензировании отдельных видов деятельности", Законом Российской Федерации "О средствах массовой информации" и иными нормативными правовыми актами, определяющими предоставление государственных услуг и исполнение государственных функций в установленной сфере ведения Роскомнадзора.

4.10. Обработка персональных данных, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, указанных в пункте 4.1 настоящего Положения, осуществляется сотрудниками структурных подразделений Управления, предоставляющими соответствующие государственные услуги и (или) исполняющими государственные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

4.11. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Управление для получения

государственной услуги или в целях исполнения государственной функции, осуществляется путем:

4.11.1. получения оригиналов необходимых документов (заявление);

4.11.2. заверения копий документов;

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

4.11.4. внесения персональных данных в прикладные программные подсистемы Единой информационной системы Роскомнадзора.

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

4.13. При предоставлении государственной услуги или исполнении государственной функции Управлением запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

4.14. При сборе персональных данных уполномоченное должностное лицо Управления, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением государственной услуги или в связи с исполнением государственной функции, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

4.15. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Управлением осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

V. Порядок обработки персональных данных субъектов персональных данных в информационных системах

5.1. Обработка персональных данных в Управлении Роскомнадзора по Брянской области осуществляется:

5.1.1. В информационной системе "1С: Предприятие";

5.1.2. На автоматизированном рабочем месте сотрудника ответственного за кадровую работу в Управлении;

5.1.3. Системой видеоконтроля, установленной на территории Управления.

5.2. "Информационная система персональных данных Роскомнадзора" (далее - ИСПДн Роскомнадзора) содержит персональные данные государственных служащих Управления, субъектов (заявителей), обратившихся в Управление в целях получения государственных услуг или в связи с исполнением государственных функций, и включает:

5.2.1. персональный идентификатор;

5.2.2. фамилию, имя, отчество субъекта персональных данных;

5.2.3. вид документа, удостоверяющего личность субъекта персональных данных;

5.2.4. серию и номер документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

5.2.5. адрес места жительства субъекта персональных данных;

5.2.6. почтовый адрес субъекта персональных данных;

- 5.2.7. контактный телефон, факс (при наличии) субъекта персональных данных;
- 5.2.8. адрес электронной почты субъекта персональных данных;
- 5.2.9. ИНН субъекта персональных данных.

5.3. Аттестованные в соответствии с законодательством Российской Федерации под обработку персональных данных автоматизированные рабочие места, входящие в состав "Единой информационной системы Роскомнадзора" (далее - АРМ ЕИС Роскомнадзора),

5. включают персональные данные субъектов, получаемые сотрудниками Управления в рамках предоставления государственных услуг и исполнения государственных функций, и включают:

- 5.3.1. персональный идентификатор;
- 5.3.2. адрес места жительства субъекта персональных данных;
- 5.3.3. почтовый адрес субъекта персональных данных;
- 5.3.4. телефон субъекта персональных данных;
- 5.3.5. факс субъекта персональных данных;
- 5.3.6. адрес электронной почты субъекта персональных данных.

5.4. Программный продукт "1С Бухгалтерия", содержит персональные данные государственных служащих Управления и физических лиц, являющихся стороной гражданско-правовых договоров, заключаемых Управлением, и включает:

- 5.4.1. фамилию, имя, отчество субъекта персональных данных;
- 5.4.2. дату рождения субъекта персональных данных;
- 5.4.3. место рождения субъекта персональных данных;

5.4.4. серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

- 5.4.5. адрес места жительства субъекта персональных данных;
- 5.4.6. почтовый адрес субъекта персональных данных;
- 5.4.7. телефон субъекта персональных данных;
- 5.4.8. ИНН субъекта персональных данных;

4.9. табельный номер субъекта персональных данных;

5.4.10. должность субъекта персональных данных;

5.4.11. номер приказа и дату приема на работу (увольнения) субъекта персональных данных.

5.5. Автоматизированное рабочее место сотрудника, отвечающего за кадровую работу в Управлении предполагают обработку персональных данных государственных служащих Управления, предусмотренных пунктом 2.2 настоящего Положения.

5.6. Классификация информационных систем персональных данных, указанных в пункте 5.1 настоящего Положения, осуществляется в порядке, установленном законодательством Российской Федерации.

5.7. Государственным служащим Управления, имеющим право осуществлять обработку персональных данных в информационных системах Управления, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным

подсистемам в соответствии с функциями, предусмотренными должностными регламентами государственных служащих Управления.

Информация может вноситься как в автоматическом режиме, при получении персональных данных с Единого портала государственных услуг или официального сайта Управления, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

5.8. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Управления, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

5.8.1. определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Управления;

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

5.8.3. применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

5.8.4. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5.8.5. учет машинных носителей персональных данных;

5.8.6. обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

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

5.8.8. установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Управления, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Управления;

5.8.9. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

5.9. Сотрудники Управления, ответственные за обеспечение информационной безопасности в Управлении, организуют и контролируют ведение учета материальных носителей персональных данных.

5.10. Сотрудники Управления, ответственные за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Управления, должны обеспечить:

5.10.1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Управлении и руководителя Управления;

5.10.2. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

5.10.3. возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.10.4. постоянный контроль за обеспечением уровня защищенности персональных данных;

5.10.5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

5.10.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

5.10.7. при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

5.10.8. разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5.11. Сотрудник Управления, ответственный за обеспечение функционирования информационных систем персональных данных в Управлении, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

5.12. Обмен персональными данными при их обработке в информационных системах персональных данных Управления осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

5.13. Доступ государственных служащих Управления к персональным данным, находящимся в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

5.14. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Управления уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

VI. Сроки обработки и хранения персональных данных

6.1. Сроки обработки и хранения персональных данных государственных служащих и работников Управления, граждан, претендующих на замещение должностей государственной службы определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных государственных служащих в соответствии с номенклатурой дел.

6.1.1. Персональные данные, содержащиеся в приказах по личному составу государственных служащих Управления (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в кадровом подразделении Управления в течение двух лет, с последующим формированием и передачей указанных документов в архив Управления или государственный архив в порядке, предусмотренном законодательством Российской Федерации.

6.1.2. Персональные данные, содержащиеся в личных делах государственных служащих Управления, а также личных карточках государственных служащих Управления, хранятся в кадровом подразделении Управления в течение десяти лет, с последующим формированием и передачей указанных документов в архив Управления или государственный архив в порядке, предусмотренном законодательством Российской Федерации.

6.1.3. Персональные данные, содержащиеся в приказах о поощрениях, материальной помощи государственных служащих Управления, подлежат хранению в течение двух лет в кадровом подразделении Управления с последующим формированием и передачей указанных документов в архив Управления или государственный архив в порядке, предусмотренном законодательством Российской Федерации.

6.1.4. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о командировках, о дисциплинарных взысканиях государственных служащих Управления, подлежат хранению в кадровом подразделении Роскомнадзора в течение пяти лет с последующим уничтожением.

6.1.5. Персональные данные, содержащиеся в документах претендентов на замещение вакантной должности государственной службы в Управлении Роскомнадзора по Брянской области, не допущенных к участию в конкурсе, и кандидатов, участвовавших в конкурсе, хранятся в кадровом подразделении Управления в течение 3 лет со дня завершения конкурса, после чего подлежат уничтожению.

6.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Управление в связи с получением государственных услуг и исполнением государственных функций, указанных в пункте 4.1 настоящего Положения, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

6.3. Персональные данные граждан, обратившихся в Управление Роскомнадзора по Брянской области лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет.

6.4. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с предоставлением Управлением государственных услуг и исполнением государственных функций, хранятся на бумажных носителях в структурных подразделениях Управления, к полномочиям которых относится обработка персональных данных в связи с предоставлением государственной услуги или исполнением государственной функции, в соответствии с утвержденными положениями Управления.

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

6.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

6.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений Управления.

6.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных Управления, указанные в пункте 5.1 настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

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

7.1. Структурными подразделениями Управления, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

7.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии Управления (далее – Комиссия), состав которой утверждается приказом Управления.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами Комиссии и утверждается руководителем Управления.

7.3. Управление в порядке, установленном законодательством Российской Федерации, определяется подрядная организация, имеющая необходимую производственную базу для обеспечения установленного порядка уничтожения документов. Должностное лицо Управления, ответственное за архивную деятельность, сопровождает документы, содержащие персональные данные, до производственной базы подрядчика и присутствует при процедуре уничтожения документов (сжигание или химическое уничтожение).

7.4. По окончании процедуры уничтожения подрядчиком и должностным лицом Управления, ответственным за архивную деятельность, составляется соответствующий Акт об уничтожении документов, содержащих персональные данные.

7.5. 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.

VIII. Рассмотрение запросов субъектов персональных данных или их представителей

8.1. Государственные служащие Управления, граждане, претендующие на замещение должностей государственной службы и подавшие документы на участие в конкурсе и лица, состоящие с ними в родстве (свойстве), обратившиеся с заявлением о предоставлении единовременной субсидии на приобретение жилого помещения, а также граждане, персональные данные которых обрабатываются в Управлении в связи с предоставлением государственных услуг и осуществлением государственных функций, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

8.1.1. подтверждение факта обработки персональных данных в Управлении;

8.1.2. правовые основания и цели обработки персональных данных;

8.1.3. применяемые в Управлении способы обработки персональных данных;

8.1.4. наименование и место нахождения Управления, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Управлением или на основании федерального закона;

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

8.1.6. сроки обработки персональных данных, в том числе сроки их хранения в Управлении;

8.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

8.1.8. информацию об осуществленной или предполагаемой трансграничной передаче данных;

8.1.9. наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Управления, если обработка поручена или будет поручена такой организации или лицу;

8.1.10. иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

8.2. Лица, указанные в пункте 8.1 настоящего Положения (далее - субъекты персональных данных), вправе требовать от Управления уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.3. Сведения, указанные в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

8.4. Сведения, указанные в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения Управления, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

8.4.1. номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

8.4.2. сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Управлением (документ, подтверждающий прием документов на участие в конкурсе на замещение вакантных должностей государственной гражданской службы, оказание Управлением государственной услуги или осуществление государственной функции), либо сведения, иным образом подтверждающие факт обработки персональных данных в Управлении, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.5. В случае, если сведения, указанные в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Управление или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.6. Субъект персональных данных вправе обратиться повторно в Управление или направить повторный запрос в целях получения сведений, указанных в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 8.5 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8.4 настоящего Положения, должен содержать обоснование направления повторного запроса.

8.7. Управление Роскомнадзора по Брянской области вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.5 и 8.6 настоящего Положения. Такой отказ должен быть мотивированным.

8.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

IX. Лицо, ответственное за организацию обработки персональных данных в Управлении Роскомнадзора по Брянской области

9.1. Ответственный за организацию обработки персональных данных в Управлении (далее - Ответственный за обработку персональных данных в Управлении) назначается руководителем Управления из числа государственных служащих, относящихся к главной группе должностей категории "руководители" Управления в соответствии с распределением обязанностей.

9.2. Ответственный за обработку персональных данных Управления в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

9.3. Ответственный за обработку персональных данных Управления обязан:

9.3.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Управлении от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

9.3.2. осуществлять внутренний контроль за соблюдением государственными служащими Управления требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

9.3.3. доводить до сведения государственных служащих Управления положения законодательства Российской Федерации в области персональных данных, локальных

актов по вопросам обработки персональных данных, требований к защите персональных данных;

9.3.4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Управлении;

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

9.4. Ответственный за обработку персональных данных вправе:

9.4.1. иметь доступ к информации, касающейся обработки персональных данных в Управлении и включающей:

9.4.1.1. цели обработки персональных данных;

9.4.1.2. категории обрабатываемых персональных данных;

9.4.1.3. категории субъектов, персональные данные которых обрабатываются;

9.4.1.4. правовые основания обработки персональных данных;

9.4.1.5. перечень действий с персональными данными, общее описание используемых в Управлении способов обработки персональных данных;

9.4.1.6. описание мер, предусмотренных статьями 18.1 и 19 Федерального закона "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

9.4.1.7. дату начала обработки персональных данных;

9.4.1.8. срок или условия прекращения обработки персональных данных;

9.4.1.9. сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

9.4.1.10. сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

9.4.2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Управлении, иных государственных служащих Управления с возложением на них соответствующих обязанностей и закреплением ответственности.

9.5. Ответственный за обработку персональных данных в Управлении несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в Управлении в соответствии с положениями законодательства Российской Федерации в области персональных данных.

ИНСТРУКЦИЯ

администратора безопасности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Управления Роскомнадзора по Брянской области

1. Общие положения

1. Настоящая инструкция регламентирует порядок работы администратора безопасности с документами, электронными и магнитными носителями, содержащими персональные данные в Управлении Роскомнадзора по Брянской области (далее – Управление) в соответствии с Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012г. N1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении положения о методах и способах защиты в информационных системах персональных данных», со специальными требованиями и рекомендациями по технической защите конфиденциальной информации утвержденными приказом Гостехкомиссии России от 30.08.2001 № 282, в соответствии с требованиями методического документа ФСТЭК “Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных” (утверждены 15 февраля 2008г).

Администратор безопасности информации - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационной системы персональных данных, предназначенных для обработки информации, содержащей персональные данные. Администратор безопасности в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в информационной системе персональных данных (далее ИСПДн). Администратор безопасности назначается установленным порядком приказом Управления. Администратор безопасности в своей работе руководствуется положениями нормативно-правовых актов РФ, нормативных актов Управления по обеспечению безопасной обработки информации и положений настоящей Инструкции.

2. Администратор безопасности обеспечивает:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрацию действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет съемных носителей информации в журналах утвержденных нормативным актом Организации, а также осуществляет их хранение и обращение, исключая хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;
- реализацию функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений в зависимости от класса информационной системы и исходя из угроз безопасности персональных данных, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа;
- контроль за межсетевым экранированием, управляет настройками фильтрации входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом) и трансляцией сетевых адресов для скрытия структуры информационной системы;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защиту информации при ее передаче по каналам связи;
- контроль за использованием сотрудниками Организации смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- централизованное управление системой защиты персональных данных информационных систем Управления;
- периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;
- активный аудит безопасности информационных систем с целью обнаружения в режиме реального времени несанкционированной сетевой активности;
- анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.
- проверку подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети (сети связи общего пользования) данных;
- осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;
- предотвращение возможности отрицания пользователем факта отправки персональных данных другому пользователю;
- предотвращение возможности отрицания пользователем факта получения персональных данных от другого пользователя;
- проверку программного обеспечения средств защиты информации, применяемых в информационных системах 1 класса, проходит контроль отсутствия недеklarированных возможностей;
- проведение контроля отсутствия недеklarированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 2 и 3 классов (при необходимости);
- при необходимости применять другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных. Перед этим поставить в известность: сотрудников обеспечивающих информационную безопасность Управления, и организацию аттестовавшую ИСПДн;
- выявление возможных каналов утечки информации и способов совершения несанкционированного доступа (далее – НСД) и принятие мер по их устранению;
- обучение и консультации пользователей ИСПДн правилам работы со средствами защиты информации в Управлении;

- контроль по установке программно-технических средств защиты информации на АРМ Управления в соответствии с установленной технологией обработки информации.

- контроль за использованием, хранением и размножением на автоматизированном рабочем месте программных продуктов и носителей информации, непосредственно не связанных со служебной деятельностью на данном рабочем месте;

- контроль за выполнением требований Аттестата соответствия требованиям по безопасности персональных данных при их обработке в ИСПДн, а при необходимости соответствие состава и расположения основных технических средств и систем и вспомогательных технических средств и систем;

- контроль за внесением несанкционированных изменений в системы электроснабжения, заземления и других проводных коммуникаций объекта;

- генерацию ключей, личных идентификаторов, а так же паролей для пользователей ИСПДн;

- учет персональных идентификаторов, ключей, карточек паролей;

- контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих средств защиты информации, с целью недопущения и выявления несанкционированных модификаций;

- корректировку содержания с целью соответствия реальным условиям настоящей Инструкции, а также нормативных документов обеспечивающих проведение мероприятий по обеспечению безопасности обработки персональных данных в Управлении;

- и разрабатывает предложения по составу общесистемных программных средств, обеспечивающих функционирование автоматизированной системы;

- контроль за действиями пользователей и обслуживающего персонала, за исполнением ими требований по обеспечению безопасности обработки информации в ИСПДн.

3. Администратор безопасности обязан:

- знать способы, методы и средства защиты информации (далее – СЗИ), обрабатываемой с использованием автоматизированной системы;

- знать перечень задач, решаемых с использованием автоматизированной системы, и пользователей, допущенных к их решению;

- 2 раза в год проводить занятия с пользователями, доводить основные положения нормативных, правовых и руководящих документов по вопросам защиты (обеспечению безопасности информации);

- еженедельно анализировать содержимое системных журналов средств защиты информации на предмет попыток НСД и 1 раз в квартал архивировать журнал СЗИ НСД;

- периодически, но не реже двух раз в год, тестировать все функции системы разграничения доступа к информации, обрабатываемой с использованием автоматизированной системы;

- осуществлять раз в месяц визуальный контроль целостности компонентов автоматизированной системы и установленных средств защиты;

- контролировать работу установленной антивирусной программы и раз в день осуществлять проверку электронного журнала учета работы антивирусной программы на наличие компьютерных «вирусов»;

- обновлять не реже одного раза в неделю антивирусные средства (базу данных), установленных на автоматизированных рабочих местах;

- контролировать правильность применения и работоспособность средств защиты информации от НСД;

- в соответствии с инструкцией по парольной защите в Управлении вести учет, хранение, закрепление и выдачу паролей доступа к техническим средствам и информационным ресурсам автоматизированной системы;
- при необходимости проведения обслуживания или ремонта средств вычислительной техники докладывать руководителю структурного подразделения ответственному за информационную безопасность в Управлении (а при его отсутствии ответственному за организацию обработки персональных данных в Управлении) и после согласования с организациями, проводившими работы по защите персональных данных и в соответствии с полученным указанием проводить работы;
- своевременно удалять описание пользователей из базы данных СЗИ при изменении списка допущенных к работе с ИСПДн лиц;
- знать работу установленных средств защиты, при необходимости проводить администраторские работы с отметкой в журнале, учитывающие работы со средствами СЗИ;
- постоянно повышать свою квалификацию;
- участвовать в мероприятиях по защите информации;
- участвовать и контролировать проведение аттестационных испытаний автоматизированной системы;
- организовывать и контролировать проведение мероприятий по резервному копированию персональных данных Управления.
- Немедленно докладывать ответственному за организацию обработки персональных данных в Управлении о фактах нарушения или невыполнения пользователями АРМ требований по защите информации и обеспечению безопасности ИСПДн.

4. Права администратора безопасности

Администратор безопасности имеет право:

- требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн;
- докладывать руководителю Управления, ответственного за эксплуатацию объекта информатизации, о нарушениях или невыполнении пользователями требований по защите (обеспечению безопасности) информации и правил обращения со съемными машинными носителями информации;
- останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования СЗИ.

1

5. Ответственность

На администратора безопасности возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

Администратор безопасности несет ответственность по законодательству Российской Федерации за нарушение требований нормативно - методических документов по защите информации и настоящей инструкции.

Ему запрещается: сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИСПДн.

Правила
обработки персональных данных, устанавливающие процедуры,
направленные на выявление и предотвращение нарушений
законодательства Российской Федерации в сфере персональных данных,
а также определяющие для каждой цели обработки персональных
данных содержание обрабатываемых персональных данных, категории
субъектов, персональные данные которых обрабатываются, сроки их
обработки и хранения, порядок уничтожения при достижении целей
обработки или при наступлении иных законных оснований

Перечень сокращений:

ПДн Персональные данные

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

НСД Несанкционированный доступ

АИС Автоматизированная информационная система

ИСПДн Информационная система персональных данных

СКЗИ Средство криптографической защиты информации

АРМ Автоматизированное рабочее место

Правила Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки

или при наступлении иных законных оснований

Управление

Управление Роскомнадзора по Брянской области

Термины и определения:

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

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

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

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

Использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом (лицами) Управления в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении сотрудников либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

Конфиденциальность персональных данных — обязанность Управления и его сотрудников не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

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

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) — обработка персональных данных соответствующая характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяющая осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

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

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

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

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

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с:

- Статьей 24 Конституции Российской Федерации;
- Главой 14 Трудового Кодекса Российской Федерации;
- Федеральным законом Российской Федерации № 152-ФЗ

«О персональных данных» от 27.07.2006;

- Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006;

- Постановлением Правительства РФ от 21.03.2012 № 211

«Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- Постановлением Правительства РФ от 01.11.2012 № 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановлением Правительства РФ от 15.09.2008 № 687

«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

- Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- Приказом Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ").

1.2. Цель разработки документа — определение порядка обработки ПДн субъектов ПДн; обеспечение защиты прав и свобод субъектов ПДн при обработке их ПДн, а также установление ответственности должностных лиц, имеющих доступ к ПДн субъектов, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

1.3. Порядок ввода в действие и изменения Правил.

1.3.1 Настоящие Правила вступают в силу с момента их утверждения Руководителем Управления и действуют бессрочно, до замены их новыми Правилами.

1.3.2 Все изменения в Правила вносятся приказом.

2. Состав, категории и содержание ПДн

2.1 Персональные данные, обрабатываемые в Управлении, относятся к сведениям конфиденциального характера (конфиденциальной информации).

2.2 В Управлении обрабатываются ПДн следующих субъектов ПДн:

- сотрудники Управления;
- субъекты ПДн, не являющиеся сотрудниками Управления.

3. Основные условия проведения обработки ПДн

3.1. Обработка ПДн осуществляется после получения согласия субъекта ПДн, за исключением случаев, предусмотренных частью 3.2 настоящих Правил.

3.2. Согласие субъекта ПДн, предусмотренное п.3.1 настоящих Правил не требуется в следующих случаях:

1) обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на Управление функций, полномочий и обязанностей;

2) обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

3) обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

4) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

5) обработка ПДн необходима для осуществления прав и законных интересов Управления или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн.

3.3. Письменное согласие субъекта ПДн должно включать:

1) фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

3) наименование или фамилию, имя, отчество и адрес Оператора;

4) цель обработки ПДн;

5) перечень ПДн, на обработку которых дается согласие субъекта ПДн;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка будет поручена такому лицу;

7) перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

8) срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта ПДн.

3.4. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных п. 3.5 настоящих Правил.

3.5. Обработка специальных категорий ПДн допускается в случаях, если:

1) субъект ПДн дал согласие в письменной форме на обработку своих ПДн;

2) ПДн сделаны общедоступными субъектом ПДн;

3) обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

4) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

5) обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;

6) обработка ПДн осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

7) обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

3.6. Лица, допущенные к обработке ПДн, в обязательном порядке под роспись знакомятся с требованиями настоящих Правил.

3.7. Запрещается:

- обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод ПДн под диктовку (голосовой ввод).

4. Обработка ПДн

Обработка ПДн подразделяется на:

- обработка ПДн в ИСПДн;
- обработка ПДн, осуществляемая без использования средств автоматизации.

4.1 Обработка ПДн в ИСПДн

4.1.1 Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

- Не допускается обработка ПДн в ИСПДн с использованием средств автоматизации, если применяемые меры и средства обеспечения безопасности не соответствуют требованиям, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012

№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

- Обработка ПДн с использованием средств автоматизации осуществляется в рамках ИСПДн Управления и внешних информационных систем, предоставляемых сторонними организациями. Состав ИСПДн Управления определяется «Перечнем информационных систем персональных данных», утверждаемым руководителем Управления.

4.2. Обработка ПДн, осуществляемая без использования средств автоматизации

4.2.1. Настоящий порядок обработки персональных данных, осуществляемой без использования средств автоматизации (далее – Порядок) конкретизирует основные особенности обработки персональных данных, содержащиеся в информационных системах персональных данных Управления Роскомнадзора по Брянской области (далее – Управление) и изложенные в Положении об обработке и защите персональных данных в Управлении Роскомнадзора по Брянской области, утвержденном приказом Управления от 26.02.2013 № 31.

4.2.2. Обработка персональных данных, содержащихся в информационных системах Управления либо извлеченных из этих систем, считается осуществленной без

использования средств автоматизации (неавтоматизированной), если такие действия, как использование, уточнение, распространение, уничтожение персональных данных, осуществляются при непосредственном участии их субъекта.

4.2.3. Сотрудники, допущенные к обработке персональных данных в информационных системах Управления, а также к обработке персональных данных, находящихся на бумажных и других нецифровых материальных носителях, должны быть ознакомлены с настоящим Порядком до начала работы, а также проинформированы в письменном виде о факте обработки ими персональных данных, обработка которых осуществляется Управлением без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами Роскомнадзора, а также локальными правовыми актами организации.

4.2.4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм.

4.2.5. При размещении персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Управлением способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку персональных данных;

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

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

4.2.7. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Управление, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала должна быть предусмотрена актом Управления, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных,

а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

4.2.8. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.2.9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4.2.10. Положения, предусмотренные пунктами 6 и 7 настоящего Порядка, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

4.2.11. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.2.12. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. Также необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. Ответственность за организацию выполнения настоящего требования на рабочих местах сотрудников возлагается на начальников отделов, которые в указанных целях организуют рабочий процесс в возглавляемых отделах и распределяют должностные обязанности и функции между сотрудниками таким образом, чтобы исключить ознакомление с обрабатываемыми персональными данными, не требующимися в работе.

4.2.13. Локальным актом Управления определяются помещения и места хранения персональных данных, порядок доступа в помещения, а также перечень лиц,

осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.2.14. Ответственным за организацию обработки персональных данных Управления осуществляется периодический и текущий контроль соблюдения условий обработки и хранения персональных данных.»

5. Основные этапы обработки ПДн

5.1. Получение ПДн

1.3.1. Управление получает ПДн непосредственно от субъекта ПДн или от законных представителей субъектов, наделенных соответствующими полномочиями.

1.3.2. Субъект ПДн обязан предоставлять Управлению достоверные сведения о себе. Управление имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися у Управления документами.

Предоставление субъектом ПДн - сотрудником Управления подложных документов или заведомо ложных сведений при заключении трудового договора является основанием для расторжения трудового договора в соответствии с пунктом 11 части первой статьи 81 Трудового кодекса Российской Федерации, а также пунктом 8 части 1 статьи 16 Федерального закона от 27.07.2004 N 79-ФЗ «О государственной гражданской службе Российской Федерации».

При изменении ПДн субъект ПДн - сотрудник Управления письменно уведомляет Управление о таких изменениях в разумный срок, не превышающий 14 дней с момента изменений. Данное обязательство не распространяется на изменение ПДн, предоставление которых требует соответствующее согласие сотрудника.

1.3.3. Если обязанность предоставления ПДн установлена федеральным законом, сотрудники Управления обязаны разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн.

5.1.4. Если ПДн получены не от субъекта ПДн, Управление, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

- 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- 2) цель обработки ПДн и ее правовое основание;
- 3) предполагаемые пользователи ПДн;
- 4) установленные федеральным законом права субъекта ПДн;
- 5) источник получения ПДн.

5.1.5. Управление освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные п. 5.1.4, в случаях, если:

- 1) субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- 2) ПДн получены Управлением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- 3) ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника.

5.2. Хранение ПДн

5.2.1. Персональные данные субъектов ПДн хранятся на материальных носителях (бумажные, электронные носители), в том числе и на внешних (съёмных) электронных носителях в ИСПДн.

5.2.2. В целях обеспечения сохранности и конфиденциальности ПДн все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только сотрудниками Управления, осуществляющими данную работу в

соответствии со своими служебными обязанностями, зафиксированными в их должностных регламентах.

5.2.3. Хранение ПДн должно происходить в порядке, исключающем их утрату или неправомерное использование.

5.2.4. При работе с документами, содержащими ПДн, запрещается оставлять их на рабочем месте или оставлять шкафы (сейфы) с данными документами открытыми (незапертыми) в случае выхода из рабочего помещения.

5.2.5. В конце рабочего дня все документы, содержащие ПДн, должны быть убраны в шкафы (сейфы).

5.2.6. Хранение документов, содержащих ПДн сотрудников Управления, должно осуществляться следующим образом:

- Личные дела сотрудников, картотеки, учетные журналы и книги учета хранятся в запирающихся шкафах;
- Трудовые книжки хранятся в негорючем сейфе;
- Бланки документов, ключи от рабочих шкафов сотрудников отдела государственной службы, кадров и правового обеспечения хранятся у ответственного лица, назначенного начальником отдела;
- Хранение ПДн субъектов ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки в соответствии со сроками хранения, определяемыми законодательством Российской Федерации и нормативными документами Управления;
- ПДн субъектов ПДн хранятся в отделах (подразделениях) Управления, которые отвечают за взаимодействие с субъектами;
- ПДн на бумажных носителях должны находиться в помещениях Управления в сейфах, металлических или запираемых шкафах, обеспечивающих защиту от несанкционированного доступа;
- Доступ к ИСПДн, содержащим ПДн, должен обеспечиваться с использованием средств защиты от несанкционированного доступа и копирования;
- Все электронные носители ПДн должны быть учтены. Учет внешних съемных электронных носителей информации, содержащих ПДн, осуществляется в подразделениях, осуществляющих обработку ПДн.

5.2.7. Сотрудник, имеющий доступ к ПДн сотрудников Управления в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей ПДн, исключающее доступ к ним третьих лиц;
- при уходе в отпуск, нахождении в служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте он обязан передать документы и иные носители, содержащие ПДн, лицу, на которое приказом или распоряжением Управления будет возложено исполнение его трудовых обязанностей.

Примечание 1. В случае если такое лицо не назначено, документы и иные носители, содержащие ПДн, передаются другому работнику, имеющему доступ к ПДн по указанию руководителя структурного подразделения.

Примечание 2. Сотрудники отдела организационной правовой работы и кадров, осуществляющие ведение личных дел сотрудников Управления, обязаны обеспечивать конфиденциальность сведений, содержащихся в личных делах сотрудников Управления.

Примечание 3. Сотрудники отдела организационной правовой работы и кадров, осуществляющие ведение личных дел сотрудников Управления, обязаны ознакомливать сотрудника Управления с документами своего личного дела не реже одного раза в год, а также по просьбе сотрудника и во всех иных случаях, предусмотренных законодательством Российской Федерации.

5.2.8. При увольнении сотрудника, имеющего доступ к ПДн, документы и иные носители, содержащие ПДн, сдаются сотрудником своему непосредственному руководителю.

5.2.9. Режим конфиденциальности ПДн снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено законом.

5.2.10. После увольнения сотрудника папка «Личное дело сотрудника» перемещается в архив уволенных сотрудников и хранится в архиве 75 лет.

5.3. Порядок учета носителей ПДн

5.3.1. В Управлении должны быть учтены все машинные и бумажные носители информации, содержащие ПДн.

5.3.2. Для организации учета машинных носителей ПДн каждому носителю присваивается учетный номер. Для этого все машинные носители должны быть промаркированы печатью или наклейкой с инвентарным номером. На носители (компакт-диски и др.), на которые наклеивание ярлыка недопустимо по техническим причинам, реквизиты ярлыка полностью наносятся на диск специальным нестираемым маркером.

5.3.3. Учет машинных носителей осуществляется по «Журналу учета машинных носителей ПДн».

5.3.4. Ежегодно необходимо проводить инвентаризацию всех носителей информации, на которых хранятся ПДн. Результаты инвентаризации должны документироваться.

5.4. Использование ПДн

5.4.1. Запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п. 5.4.2 настоящих Правил.

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

5.4.3. Управление обязано разъяснить субъекту ПДн положение принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения.

5.4.4. С документами, содержащими ПДн сотрудника, которые создаются в Управлении в период трудовой деятельности сотрудника (приказы, служебные записки и т.п.), сотрудник должен быть ознакомлен под роспись.

5.4.5. Исключение или исправление неверных или неполных ПДн сотрудников Управления осуществляют работники отдела организационной правовой работы и кадров по устному требованию сотрудника после предъявления подтверждающих документов.

5.4.6. Копии документов, являющихся основанием для исправления неверных или неполных данных ПДн сотрудников, хранятся в папке «Личное дело сотрудника».

5.5. Лицо, ответственное за организацию обработки ПДн в Управлении

5.5.1. Приказом по Управлению, назначается лицо, ответственное за организацию обработки ПДн в Управлении (далее - Ответственное лицо).

5.5.2. Ответственное лицо получает указания непосредственно от Руководителя Управления и подотчетно ему.

5.5.3. Ответственное лицо обязано:

1) осуществлять внутренний контроль за соблюдением Управлением и его сотрудниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

2) доводить до сведения сотрудников Управления положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

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

5.6. Доступ сотрудников к ПДн субъектов ПДн, обрабатываемым в Управлении

5.6.1. Сотрудники Управления получают доступ к ПДн субъектов ПДн исключительно в объеме, необходимом для выполнения своих должностных обязанностей.

5.6.2. Список сотрудников Управления, имеющих доступ к ПДн, определяется в «Перечне должностей служащих Управления Роскомнадзора по Брянской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».

5.6.3. «Перечень должностей служащих Управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным», разрабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введении новых должностей и т.п.) Ответственным лицом на основании заявок руководителей (начальников) отделов (подразделений).

5.6.4. Работнику, должность которого не включена в «Перечень должностей служащих Управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным», но которому необходим разовый или временный доступ к ПДн субъектов ПДн в связи с исполнением должностных обязанностей, распоряжением Руководителя Управления может быть предоставлен такой доступ на основании письменного мотивированного запроса непосредственного руководителя сотрудника.

5.6.5. Работник Управления получает доступ к ПДн субъектов ПДн после ознакомления и изучения требований настоящих Правил и иных внутренних нормативных документов Управления по защите персональных данных в части, его касающейся.

5.7. Доступ субъектов ПДн к ПДн, обрабатываемым в Управлении

5.7.1. Субъект ПДн имеет право на свободный доступ к своим ПДн, включая право на получение копии любой записи (за исключением случаев, когда предоставление ПДн нарушает конституционные права и свободы других лиц), содержащей его ПДн. Субъект имеет право вносить предложения по внесению изменений в свои ПДн в случае обнаружения в них неточностей.

5.7.2. Субъект ПДн – сотрудник Управления или его законный представитель, получает доступ к своим ПДн или к иной информации, касающейся обработки его ПДн по запросу в следующие подразделения:

Отдел организационной правовой работы и кадров – для выдачи документов, связанных с его трудовой деятельностью (копии приказов о приеме на работу, переводе на другую работу, увольнении с работы, выписок из трудовой книжки, справок о месте работы, периоде работы в Управлении и др.);

5.7.3. Субъект ПДн – иное физическое лицо или его законный представитель, получает доступ к своим ПДн или к иной информации, касающейся обработки его ПДн по запросу Ответственному лицу.

5.7.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного

документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Управлением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Управлением, подпись субъекта ПДн или его представителя. В случае направления запроса по почте, он должен содержать нотариально заверенную подпись субъекта ПДн или его законного представителя.

5.7.5. Субъект ПДн имеет право на получение при обращении информации, касающейся обработки его ПДн, в том числе содержащей:

- 1) подтверждение факта обработки ПДн Управлением;
- 2) правовые основания и цели обработки ПДн;
- 3) цели и применяемые Управлением способы обработки ПДн;
- 4) наименование и место нахождения Управления, сведения о лицах (за исключением сотрудников Управления), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;
- 7) порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Управления, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные федеральными законами.

5.7.6. Уполномоченные лица обязаны сообщить субъекту ПДн или его законному представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с ними при обращении субъекта ПДн или его законного представителя не позднее тридцати рабочих дней с даты получения запроса субъекта ПДн или его законного представителя.

5.7.7. Ответ в адрес субъекта ПДн может быть направлен через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под роспись).

5.7.8. В случае отказа в предоставлении субъекту ПДн или его законному представителю при обращении либо при получении запроса субъекта ПДн или его законного представителя информации о наличии ПДн о соответствующем субъекте ПДн, а также таких ПДн, уполномоченные лица обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта ПДн или его законного представителя, либо с даты получения запроса субъекта ПДн или его законного представителя.

5.7.9. Мотивированный ответ в адрес субъекта ПДн может быть направлен через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под роспись).

5.7.10. В случае отзыва субъектом ПДн согласия на обработку его ПДн Управление обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) в срок, не превышающий

тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Управлением и субъектом ПДн, либо если Управление не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

5.7.11. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Управление обязано осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Управление обязано осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

5.7.12. В случае подтверждения факта неточности ПДн Управление на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязано уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

5.7.13. В случае выявления неправомерной обработки ПДн, осуществляемой Управлением или лицом, действующим по поручению Управления, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Управления. В случае, если обеспечить правомерность обработки ПДн невозможно, Управление в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Управление обязано уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

5.7.14. В случае достижения цели обработки ПДн Управление обязано прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Управления) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Управлением и субъектом ПДн, либо если Управление не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

5.7.15. Передача (обмен и т.д.) ПДн между отделами (подразделениями) Управления осуществляется только между сотрудниками, имеющими доступ к ПДн субъектов.

5.7.16. При передаче ПДн субъекта сотрудники, осуществляющие передачу, предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

5.7.17. Допуск к ПДн сотрудников Управления, не имеющих надлежащим образом

оформленного разрешения, запрещается.

5.8. Регламент обмена/выдачи информации (ПДн субъекта) третьим лицам (физическим и юридическим)

5.8.1. К числу внешних потребителей ПДн Управления в соответствии с нормами действующего законодательства относятся государственные органы:

- налоговые органы;
- правоохранительные органы;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- банк, в который Управление осуществляет перечисление заработной платы в соответствии с заявлением сотрудника;
- судебные органы по запросу субъекта ПДн.

5.8.2. При передаче ПДн субъекта уполномоченные лица должны придерживаться следующих требований:

- Передача ПДн субъекта третьим лицам осуществляется только с письменного согласия субъекта, за исключением случаев, установленных федеральными законами;
- Не допускается передача ПДн субъекта в коммерческих целях без его письменного согласия;
- Передача ПДн по телефону запрещается;
- Сотрудникам Управления, имеющим доступ к ПД, запрещена запись, хранение и вынос за пределы Управления на внешних носителях информации (диски, дискеты, USB флэш-карты и т.п.), передача по внешним адресам электронной почты или размещение в сети Интернет информации, содержащей ПДн субъектов, за исключением случаев, указанных в настоящих Правилах или установленных иными внутренними документами Управления;
- Передача третьим лицам документов (иных материальных носителей), содержащих ПДн субъектов, осуществляется по письменному запросу третьего лица на предоставление ПДн субъекта. Ответы на письменные запросы даются на бланке Управления и в том объеме, который позволяет не разглашать излишних сведений о субъекте ПДн;
- Работники Управления, передающие ПДн субъектов третьим лицам, должны передавать их с обязательным уведомлением лица, получающего эти документы, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена, и с предупреждением об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами. Уведомление и предупреждение могут быть реализованы путем подписания акта передачи носителей ПДн, в котором приведены указанные условия;
- Представителю субъекта (в том числе адвокату) ПДн передаются в порядке, установленном действующим законодательством и настоящим документом. Информация передается при наличии одного из документов:
 - нотариально удостоверенной доверенности представителя субъекта;
 - письменного заявления субъекта, написанного в присутствии уполномоченного сотрудника (если заявление написано субъектом не в его присутствии, то оно должно быть нотариально заверено);
- Предоставление ПДн субъекта государственным органам производится в соответствии с требованиями действующего законодательства Российской Федерации;
- ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда

передача ПДн субъекта без его согласия допускается действующим законодательством РФ;

- Документы, содержащие ПДн субъекта, могут быть отправлены посредством федеральной почтовой связи заказным письмом. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие ПДн, вкладываются в конверт, в документах делается надпись о том, что ПДн, содержащиеся в письме, являются конфиденциальной информацией и не подлежат распространению и (или) опубликованию. Лица, виновные в нарушении требований конфиденциальности, несут ответственность, предусмотренную законодательством Российской Федерации.

5.8.3. Учет переданных ПДн осуществляется в рамках принятых в Управлении правил делопроизводства путем регистрации входящей и исходящей корреспонденции и запросов, как государственных органов, так и структурных подразделений Управления о предоставлении ПДн физических (юридических) лиц либо их представителей. Фиксируются сведения о лицах, направивших такие запросы, дата выдачи ПДн, а также дата уведомления об отказе в предоставлении ПДн (в случае отказа).

5.8.4. В случае, если лицо, обратившееся в Управление с запросом на предоставление ПДн, не уполномочено на получение информации, относящейся к ПДн, уполномоченные лица Управления обязаны отказать данному лицу в выдаче такой информации. Лицу, обратившемуся с соответствующим запросом, выдается уведомление в свободной форме об отказе в выдаче информации, а копия уведомления хранится в соответствии с принятыми правилами делопроизводства (как исходящая корреспонденция). В случае, если запрашивались ПДн сотрудника Управления, копия уведомления также подшивается в личное дело сотрудника, ПДн которого не были предоставлены.

5.9. Уничтожение ПДн

5.9.1. ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.9.2. Уничтожение ПДн, не подлежащих архивному хранению, осуществляется только комиссией в составе представителя подразделения (или сотрудника), ответственного за защиту ПДн и представителя структурного подразделения, в чьем ведении находятся указанные ПДн. По результатам уничтожения должен оформляться Акт.

6. Ответственность

6.1. С правилами работы и хранения конфиденциальной информации о ПДн в обязательном порядке должны быть ознакомлены все работники Управления, подписав лист ознакомления с настоящими Правилами.

6.2. Сотрудник, которому в силу трудовых отношений с Управлением стала известна информация, составляющая ПДн, в случае нарушения режима защиты этих ПДн несет материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

6.3. Разглашение ПДн субъектов ПДн (передача их посторонним лицам, в том числе сотрудникам Управления, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих ПДн субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящими Правилами, локальными нормативными актами (приказами, распоряжениями) Управления, может повлечь наложение на сотрудника, имеющего доступ к ПДн, дисциплинарного взыскания, если иное не предусмотрено законодательством РФ.

6.4. Сотрудник Управления, имеющий доступ к ПДн субъектов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в

случае причинения его действиями ущерба Управлению (п.7 ст.243 Трудового кодекса РФ).

6.5. Сотрудники Управления, имеющие доступ к ПДн субъектов, виновные в незаконном разглашении или использовании ПДн субъектов без согласия субъектов из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут ответственность в соответствии с законодательством РФ.

6.6. Руководство Управления за нарушение норм, регулирующих получение, обработку и защиту ПДн сотрудника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей ПДн сотрудника.

7. Дополнительные положения

7.1 Каждый сотрудник должен быть ознакомлен с настоящими Правилами под роспись при приеме на работу, а для сотрудников, принятых ранее даты его утверждения, не позднее 1 (одного) месяца с даты утверждения настоящих Правил.

7.2 Настоящие Правила хранятся в отделе организационной правовой работы и кадров Управления, контролируемые копии хранятся в информационных системах Управления.

Правила рассмотрения запросов субъектов персональных данных или их представителей

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

Оператор – Управление Роскомнадзора по Брянской области, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных в отношении себя, а также на ознакомление с такими персональными данными.

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

3. Сведения о наличии персональных данных должны быть представлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4. Доступ к своим персональным данным представляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с действующим законодательством Российской Федерации.

Законный представитель представляет оператору документ, подтверждающий его полномочия.

5. Субъект персональных данных имеет право на получение при обращении к оператору, следующих сведений:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального законодательства Российской Федерации;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством Российской Федерации;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами Российской Федерации.

6. Если запрос субъекта персональных данных связан с внесением изменений в персональные данные субъекта в связи с тем, что персональные данные, обрабатываемые оператором, являются неполными, устаревшими, недостоверными, то в таком запросе субъект персональных данных должен указать какие именно персональные данные изменяются или уточняются.

Если для внесения изменений в персональные данные необходимы подтверждающие документы, то субъект персональных данных прикладывает к своему запросу об изменении персональных данных доказательства, на основании которых оператор должен внести изменения или уточнить персональные данные.

В случае отсутствия доказательств, на которые ссылается субъект персональных данных, оператор оставляет персональные данные в неизменном виде. Внесение изменений или уточнение персональных данных оператором должны быть выполнены в течение 7 рабочих дней со дня предоставления таких сведений.

Изменения, уничтожение или блокирование персональных данных соответствующего субъекта осуществляется оператором на безвозмездной основе.

Правила
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных,
установленным федеральным законом "о персональных данных",
принятыми в соответствии с ним нормативными правовыми актами и
локальными актами Управления Роскомнадзора по Брянской области

Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом

«О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152 «О персональных данных».

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Управлении Роскомнадзора по Брянской области (далее – Управление) организовывается проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в Управлении либо комиссией, созданной на основании Приказа руководителя Управления.

В проведении проверки не может участвовать сотрудник Управления, прямо или косвенно заинтересованный в ее результатах.

Проверки соответствия обработки персональных данных установленным требованиям в Управлении проводятся на основании утвержденного руководителем Управления ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

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

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

- порядок ознакомления лиц с локальными актами оператора;
- перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ;
- соблюдение правил доступа к персональным данным;
- соблюдение условий хранения персональных данных;
- своевременность уничтожения персональных данных по достижению цели;
- 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, обрабатываемых в информационной системе персональных данных;
- состояние учета машинных носителей персональных данных;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- осуществление мероприятий по обеспечению целостности персональных данных.

Ответственный за организацию обработки персональных данных в Управлении (члены комиссии) имеет право:

запрашивать у сотрудников Управления информацию, необходимую для реализации полномочий;

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

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

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

представлять руководителю Управления предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных (членам комиссии) в Управлении в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. По результатам проведенной проверки составляется Акт, в котором указывается перечень мер, необходимых для устранения выявленных нарушений.

Правила работы с обезличенными данными

1. Термины и определения

Перечень сокращений:

ПДн Персональные данные

НСД Несанкционированный доступ

АИС Автоматизированная информационная система

ИСПДн Информационная система персональных данных

Управление Управление Роскомнадзора по Брянской области

В рамках данного документа используются следующие термины и определения:

Доступ к информации – возможность получения информации и ее использования.

Защита информации от несанкционированного доступа (защита от НСД) или воздействия – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

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

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

АИС Управления – объединение информационных систем, в том числе информационных систем персональных данных, компьютерного, телекоммуникационного и офисного оборудования всех отделов (подразделений) Управления, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Нарушение информационной безопасности – событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность или целостность).

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись,

систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Пользователь информационной системы – сотрудник Управления (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в АИС Управления в установленном порядке.

2. Общие положения

Настоящие Правила работы с обезличенными персональными данными Управления разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" (с приложением «Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ») и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

3. Порядок работы с обезличенными ПДн

Обезличивание должно обеспечивать не только защиту ПДн от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых ПДн.

К свойствам обезличенных данных относятся:

- полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имела до обезличивания);
- структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);
- релевантность (возможность обработки запросов по обработке ПДн и получения ответов в одинаковой семантической форме);
- семантическая целостность (сохранение семантики ПДн при их обезличивании);
- применимость (возможность решения задач обработки ПДн, стоящих перед оператором, осуществляющим обезличивание ПДн, обрабатываемых в ИСПДн, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (далее - оператор, операторы), без предварительного деобезличивания всего объема записей о субъектах);
- анонимность (невозможность однозначной идентификации субъектов ПДн, полученных в результате обезличивания, без применения дополнительной информации).

К характеристикам (свойствам) методов обезличивания ПДн (далее - методы обезличивания), определяющим возможность обеспечения заданных свойств обезличенных данных, относятся:

- обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду,

позволяющему определить принадлежность ПДн конкретному субъекту, устранить анонимность);

- вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);
- изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);
- стойкость (стойкость метода к атакам на идентификацию субъекта ПДн);
- возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);
- совместимость (возможность интеграции ПДн, обезличенных различными методами);
- параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);
- возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

Требования к методам обезличивания подразделяются на:

- требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;
- требования к свойствам, которыми должен обладать метод обезличивания.

К требованиям к свойствам получаемых обезличенных данных относятся:

- сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых ПДн);
- сохранение структурированности обезличиваемых ПДн;
- сохранение семантической целостности обезличиваемых ПДн;
- анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания как, например, k-anonymity).

К требованиям к свойствам метода обезличивания относятся:

- обратимость (возможность проведения деобезличивания);
- возможность обеспечения заданного уровня анонимности;
- увеличение стойкости при увеличении объема обезличиваемых ПДн.

Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки ПДн.

Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

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

При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используются);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

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

4. Ответственность

Ответственность за осуществление общего контроля выполнения требований настоящих Правил несет ответственный за организацию обработки ПДн в Управлении.

Ответственность за поддержание данного документа в актуальном состоянии несет председатель Постоянно действующей технической комиссии Управления.

Ответственность за доведение положений настоящего документа до всех сотрудников Управления, задействованных в обработке ПДн и иных лиц в части их касающейся, а также контроль соблюдения требований документа возлагается на начальников отделов (руководителей структурных подразделений) Управления.

Ответственность за выполнение настоящих Правил возлагается на всех сотрудников Управления, допущенных к обработке ПДн.

Сотрудник Управления несёт ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования учетной записи другими лицами при соблюдении пользователем требований настоящих Правил.

Сотрудники Управления несут персональную ответственность за ущерб, причиненный Управлению и субъектам ПДн вследствие нарушения ими установленных требований в области обработки и обеспечения защиты ПДн, в соответствии с законодательством Российской Федерации.

На основании Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» сотрудники, нарушающие требования настоящих Правил, могут быть подвергнуты дисциплинарным взысканиям и увольнению с работы за неоднократное грубое нарушение Правил работы в АИС Управления (ИСПДн Управления).

Приложение N 8
к приказу Управления Роскомнадзора
по Брянской области
от 9 октября 2020 г. N 79

Персональные данные в Управлении Роскомнадзора по Брянской области обрабатываются в следующих информационных системах персональных данных (ИСПДн):

Перечень информационных систем персональных данных

| № п/п | Наименование ИСПДн | Перечень автоматизированных систем, входящих в ИСПДн | Категория обрабатываемых ПДн | Тип ИСПДн | Класс ИСПДн |
|----------|-------------------------|--|---|---|-------------------|
| 1 | ИСПДн «1С: Предприятие» | «1С:Предприятие 8» | Персональные данные, которые помимо идентификации субъекта персональных данных, позволяют получить о нем дополнительную информацию. | Локальная ИС «Бухгалтерия» многопользовательская, с разграничением прав доступа пользователей, без использования технологии удаленного доступа. | К3 специальная |
| 2 | ИСПДн ЕИСУКС | ЕИСУКС | Персональные данные, которые помимо идентификации субъекта персональных данных, позволяют получить о нем дополнительную информацию. | Однопользовательская локальная ИС с разграничением прав доступа пользователей, без использования технологии удаленного доступа. | К3 специальная |

**Перечень персональных данных, обрабатываемых в Управлении
Роскомнадзора по Брянской области в связи с реализацией служебных и
трудовых отношений, а также в связи с оказанием государственных
услуг и осуществлением государственных функций**

**1) При обработке данных государственных гражданских служащих и работников
Управления:**

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- номер основного документа, удостоверяющего личность;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- данные свидетельства о рождении детей;
- адрес регистрации;
- адрес проживания;
- семейное положение;
- сведения об образовании;
- данные документа об образовании;
- сведения о профессии;
- сведения о трудовой деятельности;
- сведения о воинской обязанности;
- данные заграничного паспорта;
- данные страхового свидетельства обязательного пенсионного страхования;
- сведения об имущественном положении;
- сведения о доходах;
- сведения о присвоении классного чина;
- сведения о наградах;
- сведения о документах, дающих право на получение льготы;
- ИНН;
- номер телефона;
- фотографическое изображение.

2) При оказании госуслуг:

- фамилия, имя, отчество;
- гражданство;
- адрес проживания;
- наименование организации;
- паспортные данные;
- СНИЛС;
- номер телефона;
- наличие второго гражданства.

3) При исполнении государственных функций и полномочий:

- фамилия, имя, отчество;
- гражданство;
- адрес проживания;
- наименование организации;

- паспортные данные;
- СНИЛС;
- номер телефона;
- наличие второго гражданства.

**Перечень должностей служащих Управления Роскомнадзора по
Брянской области, ответственных за проведение мероприятий
по обезличиванию обрабатываемых персональных данных**

В рамках реализации требований Федерального закона от 27 июля 2006 г № 152-ФЗ «О персональных данных» и Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» в Управлении Роскомнадзора по Центральному федеральному округу утверждается «Перечень должностей служащих Управления Роскомнадзора по Брянской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных».

| Руководство | |
|---|--|
| 1 | Заместитель руководителя, ответственный за организацию обработки персональных данных |
| Отдел организационной, финансовой, правовой работы и кадров | |
| 2 | Начальник отдела (администратор безопасности) |

По мере возникновения необходимости настоящий перечень подлежит своевременной корректировке.

**Перечень должностей служащих и работников Управления
Роскомнадзора по Брянской области, замещение которых
предусматривает осуществление обработки персональных данных либо
осуществление доступа к персональным данным**

| Руководство | |
|---|---|
| 1 | Руководитель |
| 2 | Заместитель руководителя – начальник отдела |
| 3 | Помощник руководителя |
| Отдел организационной, финансовой, правовой работы и кадров | |
| 4 | Начальник отдела |
| 5 | Заместитель начальника отдела - главный бухгалтер |
| 6 | Ведущий специалист-эксперт |
| 7 | Делопроизводитель |
| 8 | Специалист по охране труда |
| Отдел контроля и надзора в сфере связи | |
| 9 | Начальник отдела |
| 10 | Главный специалист-эксперт |
| 11 | Ведущий специалист-эксперт |
| Отдел по защите прав субъектов персональных данных | |
| 12 | Начальник отдела |
| 13 | Главный специалист-эксперт |
| 14 | Ведущий специалист-эксперт |
| 15 | Специалист-эксперт |
| Отдел контроля и надзора в сфере массовых коммуникаций | |
| 16 | Ведущий специалист-эксперт |
| 17 | Специалист-эксперт |
| 18 | Делопроизводитель |

**Должностной регламент ответственного за организацию обработки
персональных данных в Управлении Роскомнадзора
по Брянской области**

Ответственный за организацию обработки персональных данных обязан:

1. Организовать предоставление субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных.
2. Осуществлять внутренний текущий контроль за соблюдением требований законодательства Российской Федерации в сфере персональных данных в Управлении Роскомнадзора по Брянской области при обработке персональных данных, в том числе требований к защите персональных данных.
3. Доводить до сведения лиц, допущенных к обработке персональных данных, положения федерального законодательства Российской Федерации о персональных данных, нормативных правовых актов Управления Роскомнадзора по Брянской области по вопросам обработки персональных данных, требований к защите персональных данных.
4. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.
5. Организовать получение обязательства о прекращении обработки персональных данных у лиц, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ним договора (контракта).
6. Организовать получение согласия на обработку персональных данных у субъектов персональных данных (при необходимости).
7. Организовать разъяснение субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

Приложение N 13
к приказу Управления Роскомнадзора
по Брянской области
от 9 октября 2020 г. N 79

Типовое обязательство служащего (работника) Управления Роскомнадзора по Брянской области, 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)

(должность)

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

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

Ответственность, предусмотренная Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

« _____ » _____ 20 ____ г. _____ / _____ /
(дата) (подпись) (фамилия и инициалы)

Форма согласия на обработку персональных данных служащих (работников) Управления Роскомнадзора по Брянской области, иных субъектов персональных данных.

Я, _____
(Фамилия, Имя, Отчество)

зарегистрирован по адресу: _____

основной документ, удостоверяющий личность:

паспорт _____ выдан _____
(серия, номер) (сведения о дате выдаче и выдавшем органе)

даю согласие оператору: Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Брянской области, ул. Карла Маркса, д. 9, г. Брянск, 241050.

с целью приема на работу в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Брянской области, внесение сведений в ИСПДн «1С: Бухгалтерия» (начисление заработной платы), Сбербанк Бизнес Онлайн (перечисление заработной платы), портал ЕИСУКС (внесение данных о сотруднике) на обработку моих персональных данных:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- номер основного документа, удостоверяющего личность;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- данные свидетельства о рождении детей;
- адрес регистрации;
- адрес проживания;
- семейное положение;
- сведения об образовании;
- данные документа об образовании;
- сведения о профессии;
- сведения о трудовой деятельности;
- сведения о воинской обязанности;
- данные заграничного паспорта;
- данные страхового свидетельства обязательного пенсионного страхования;
- сведения об имущественном положении;
- сведения о доходах;
- сведения о присвоении классного чина;
- сведения о наградах;
- сведения о документах, дающих право на получение льготы;
- ИНН;
- номер телефона;
- фотографическое изображение.

Адрес оператора, осуществляющего обработку ПДн по поручению: ПАО «Сбербанк России» 117997, Россия, Москва, ул. Вавилова, д. 19, с целью изготовления и выпуска банковской карты.

Оператор вправе осуществлять все действия (операции) с моими персональными данными, включая сбор, запись, систематизацию, накопление, хранение, обновление,

изменение, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать персональные данные любым способом с использованием средств автоматизации, а так же без таковых.

Срок в течение, которого действует согласие на обработку персональных данных - 75 лет.

Я оставляю за собой право отозвать свое согласие на обработку персональных данных путем направления письменного заявления Оператору.

" " 20__ г.

(подпись)

(ФИО)

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

Мне, _____

(Фамилия Имя Отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные Управлению Роскомнадзора по Центральному федеральному округу.

В соответствии со статьями 26, 42 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30 мая 2005 г. № 609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить Управлению Роскомнадзора по Центральному федеральному округу в связи с поступлением или прохождением государственной гражданской службы.

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

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

" " 20 г.
(дата)

(подпись)

(ФИО)

**Типовая форма разъяснения субъекту персональных данных
(замещающему должности обеспечивающего персонала) юридических
последствий отказа предоставить свои персональные данные.**

Мне, _____
(Фамилия, Имя, Отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные
Управлению Роскомнадзора по Центральному федеральному округу.

В соответствии со статьями 57, 65, 69 Трудового кодекса Российской Федерации
субъект персональных данных, поступающих на работу или работающий в Управлении
Роскомнадзора по Центральному федеральному округу, обязан представить определенный
перечень информации о себе.

Без представления субъектом персональных данных обязательных для заключения
трудового договора сведений, трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской
Федерации трудовой договор прекращается вследствие нарушения установленных
обязательных правил его заключения, если это нарушение исключает возможность
продолжения работы.

" " _____ 20__ г.
(дата)

(подпись)

(ФИО)

**Порядок доступа
сотрудников Управления Роскомнадзора по Брянской области в
помещения, в которых ведется обработка персональных данных**

Порядок доступа служащих Управления Роскомнадзора по Брянской области в помещения, в которых ведется обработка персональных данных.

1. Персональные данные относятся к категории конфиденциальной информации. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2. Список сотрудников, допущенных к обработке персональных данных, утверждается руководителем Управления Роскомнадзора по Брянской области.

3. Порядок определяет правила доступа в помещения, где хранятся и обрабатываются персональные данные, в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении персональных данных.

4. В помещения, где размещены материальные носители информации, содержащие персональные данные, допускаются только сотрудники Управления Роскомнадзора по Брянской области, имеющие доступ к персональным данным.

5. Сотрудники, имеющие доступ к персональным данным, не должны:

- оставлять в свое отсутствие незапертым помещение, в котором размещены технические средства, позволяющие осуществлять обработку персональных данных;
- оставлять в помещении посторонних лиц, не имеющих доступа к персональным данным в данном структурном подразделении, без присмотра.

6. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим обеспечивается:

- оснащением помещения охранной и пожарной сигнализацией;
- обязательным запиранием помещения на ключ, даже при выходе из него в рабочее время;
- отдельным хранением дубликатов ключей;
- закрытием шкафов и металлических сейфов, где хранятся носители информации, содержащие персональные данные.

7. Ответственность за несоблюдение Порядка несут начальники отделов (структурных подразделений) Управления Роскомнадзора по Брянской области, в которых ведется обработка персональных данных и осуществляется их хранение.

8. Внутренний контроль за соблюдением в Управлении Роскомнадзора по Брянской области порядка доступа в помещения, в которых ведется обработка персональных данных, требованиям к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Управления Роскомнадзора по Брянской области».

**Лист ознакомления
с локальными актами Управления Роскомнадзора по Брянской области,
направленными на обеспечение выполнения обязанностей,
предусмотренных
Федеральным законом «О персональных данных»**

Я, _____
(Фамилия, Имя Отчество)

подтверждаю, что ознакомлен(а) с действующими на момент подписания версиями
нижеприведенных локальных нормативных правовых актов Управления Роскомнадзора
по Брянской области:

| № п/п | Локальные нормативные акты* | Дата ознакомления | Подпись |
|----------|--|----------------------|---------|
| 1. | Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований | | |
| 2. | Правила рассмотрения запросов субъектов персональных данных или их представителей | | |
| 3. | Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами Управления Роскомнадзора по Брянской области | | |
| 4. | Правила работы с обезличенными данными | | |
| 5. | Порядок доступа служащих Управления Роскомнадзора по Брянской области в помещения, в которых ведется обработка персональных данных | | |
| 6. | Перечень должностей служащих Управления Роскомнадзора по Брянской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа | | |

| № п/п | Локальные нормативные акты* | Дата ознакомления | Подпись |
|----------|--|----------------------|---------|
| | к персональным данным | | |
| 7. | Перечень должностей служащих Управления Роскомнадзора по Брянской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных | | |

* данная форма дополняется вновь изданными локальными нормативными актами, а утратившие силу локальные нормативные акты из нее исключаются

Список должностных лиц, имеющих доступ к персональным данным и личным делам государственных гражданских служащих и работников Управления

1. Руководитель Управления;
2. Заместитель руководителя Управления – начальник отдела;
3. Начальники структурных подразделений в части личных дел сотрудников отдела;
4. Государственные гражданские служащие и работники Управления к своим персональным данным.