

1649

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ
НАУЧНО - ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО
(ФГУП НИИР)**

П Р И К А З

«27» 03 2015 г.

Москва

№ 56-П

Об утверждении Положения о порядке обработки и обеспечении безопасности персональных данных работников ФГУП НИИР

В целях определения порядка получения, обработки и передачи персональных данных работников ФГУП НИИР, а также усиления мер, направленных на защиту персональных данных, обрабатываемых в ФГУП НИИР, приказываю:

1. Утвердить прилагаемое Положение о порядке обработки и обеспечении безопасности персональных данных работников ФГУП НИИР (далее Положение).
2. Директорам филиалов ФГУП НИИР-ЛОНИИР, ФГУП НИИР-СОНИИР, ИЦ "Омега", руководителям структурных подразделений ознакомить работников ФГУП НИИР с Положением под роспись и обеспечить выполнение его требований.
3. Признать утратившим силу приказ от 21.02.2013 № 38-П "Об утверждении Положения о персональных данных работников ФГУП НИИР".
4. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор

В.В. Бутенко

Д.Г. Фокин
2183



УТВЕРЖДЕНО
приказом ФГУП НИИР
от 27.05.15 № 56-П

**ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБРАБОТКИ И ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ФГУП НИИР**

Содержание

Содержание.....	2
Термины и определения	3
I. Общие положения.....	4
II. Основные принципы обеспечения мер информационной безопасности при обработке персональных данных.....	4
III. Основные условия обработки персональных данных работников ФГУП НИИР	5
IV. Основные меры обеспечения безопасности персональных данных работников ФГУП НИИР .	6
V. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации	6
VI. Порядок обработки персональных данных без использования средств автоматизации	7
VII. Требования к обезличиванию персональных данных	9
VIII. Ответственность должностных лиц	10

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе использованы следующие термины и определения:

1. **Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
2. **Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
3. **Несанкционированный доступ (НСД)** (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному назначению и техническим характеристикам.
4. **Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
5. **Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
6. **Обработка персональных данных без использования средств автоматизации (неавтоматизированная)** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных осуществляются при непосредственном участии человека.
7. **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
8. **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.
9. **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
10. **Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
11. **Работники** - субъекты, связанные с работодателем трудовыми отношениями.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке обработки и обеспечении безопасности персональных данных работников ФГУП НИИР (далее – Положение) определяет основные требования и рекомендации по обеспечению защиты персональных данных при их обработке с использованием средств автоматизации так и без них.

1.2. Данное положение распространяется на все структурные подразделения ФГУП НИИР и его филиалы (далее - ФГУП НИИР).

1.3. Настоящим положением определяется порядок получения, обработки, передачи персональных данных работников ФГУП НИИР, а также порядок ведения их личных дел.

1.4. Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных работников ФГУП НИИР.

II. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

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

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

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

2.5. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

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

III. ОСНОВНЫЕ УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ФГУП НИИР

3.1. При обработке персональных данных работников ФГУП НИИР необходимо соблюдение следующих условий:

3.1.1. К обработке персональных данных допускаются только лица, ознакомленные с настоящим положением. Перечень лиц, допущенных к обработке персональных данных, утверждается генеральным директором ФГУП НИИР (директором филиала).

3.1.2. Обработка персональных данных осуществляется только с письменного согласия субъекта персональных данных (приложение № 1), за исключением случаев, предусмотренных постановлением Правительства Российской Федерации от 15.09.2008 № 687.

3.1.3. Лица, допущенные к обработке персональных данных, в обязательном порядке подписывают обязательство о неразглашении информации, содержащей персональные данные (приложение № 2).

3.1.4. Обработка персональных данных осуществляется в соответствии с трудовым законодательством, в целях трудоустройства и продвижения по службе работников ФГУП НИИР.

3.1.5. Информация о персональных данных предоставляется работником лично. Получение персональных данных работника у третьей стороны возможно только после письменного уведомления работника не менее чем за три рабочих дня и после получения письменного согласия работника. В письменном уведомлении руководство ФГУП НИИР должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствия отказа работника дать письменное согласие на их получение.

3.1.6. Обработка персональных данных работника, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и частной жизни не допускается.

3.1.7. Исключительно автоматизированная обработка персональных данных работников ФГУП НИИР не допускается.

3.2. При поступлении на работу работник представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальной подготовки;
- в отдельных случаях, с учетом специфики работы, действующим законодательством РФ может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

3.3. Запрещается требовать от лица, поступившего на работу, документы помимо предусмотренных Трудовым кодексом Российской Федерации, иными нормативно-правовыми актами Российской Федерации.

3.4. В целях информационного обеспечения могут создаваться доступные для работников ФГУП НИИР источники персональных данных (в том числе справочники, электронные базы).

IV. ОСНОВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ФГУП НИИР

4.1. Доступ к персональным данным работников ФГУП НИИР должен иметь ограниченный перечень лиц, утверждаемый генеральным директором ФГУП НИИР (директором филиала).

4.2. Работники, осуществляющие обработку персональных данных, должны иметь доступ к тем категориям персональных данных, которые необходимы им для выполнения своих должностных обязанностей.

4.3. В ФГУП НИИР должны быть определены перечень помещений и списки лиц, допущенных в них, утверждаемые генеральным директором ФГУП НИИР (директорами филиалов), где разрешена обработка и хранение персональных данных и носителей персональных данных (в том числе резервных).

4.4. В ФГУП НИИР должен быть определен и утвержден генеральным директором ФГУП НИИР перечень персональных данных работников, обрабатываемых в ФГУП НИИР.

4.5. Передача персональных данных в пределах ФГУП НИИР, в том числе с использованием носителей персональных данных, должна осуществляться в соответствии с требованиями настоящего Положения.

4.6. При обработке персональных данных запрещается:

4.6.1. Осуществлять обработку персональных данных в присутствии лиц, к ним не допущенных.

4.6.2. Осуществлять передачу персональных данных за пределы контролируемой зоны ФГУП НИИР (в том числе и между филиалами) способом, не согласованным с отделом ЗИ ПДТР.

4.6.3. Осуществлять передачу персональных данных работников ФГУП НИИР в другие организации, в том числе трансграничную, без письменного согласия работника, данные которого подлежат передаче, за исключением случаев, предусмотренных нормативными правовыми актами Российской Федерации.

4.6.4. Запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу возможности выполнения работником должностных обязанностей.

4.6.5. Осуществлять хранение персональных данных уволенных сотрудников сроком, превышающим требования нормативных правовых актов Российской Федерации.

4.7. Уничтожение персональных данных работников ФГУП НИИР должно происходить комиссией, состав которой утверждается генеральным директором ФГУП НИИР (директорами филиалов), методом, исключающим их дальнейшую обработку любым способом. По факту уничтожения персональных данных составляется соответствующий акт.

V. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

5.1. Обработка персональных данных в информационных системах персональных данных (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», а также с учетом приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

5.2. Для каждой ИСПДн в ФГУП НИИР должен быть определен уровень защищенности и класс автоматизированной системы, о чем составлен и утвержден генеральным директором ФГУП НИИР (директором филиала) акт классификации ИСПДн. Акт классификации составляется комиссией по классификации автоматизированных и информационных систем, состав которой утверждается генеральным директором ФГУП НИИР (директором филиала).

5.3. В ФГУП НИИР должен быть назначен администратор безопасности, отвечающий за функционирование систем защиты конкретной ИСПДн.

5.4. Средства защиты, используемые в ИСПДн, должны быть сертифицированы.

5.5. В каждой ИСПДн должны быть реализованы следующие организационные и технические меры:

5.5.1. Предотвращающие несанкционированный доступ к персональным данным работников ФГУП НИИР.

5.5.2. Препятствующие несанкционированному копированию, передаче и модификации персональных данных работников ФГУП НИИР.

5.5.3. Организующие антивирусную защиту элементов ИСПДн.

5.5.4. Организующие правила разграничения доступа к персональным данным, обрабатываемым в ИСПДн.

5.5.5. Организующие резервное копирование и сохранность информации в случае выхода из строя элементов ИСПДн.

5.6. С целью определения конкретных мер по защите персональных данных администратором безопасности составляется модель актуальных угроз для конкретной ИСПДн. Модель угроз утверждается генеральным директором ФГУП НИИР (директором филиала).

5.7. В ФГУП НИИР должен быть определен и утвержден генеральным директором (директором филиала) список лиц, имеющих право доступа в ИСПДн. Для каждого сотрудника ФГУП НИИР, имеющего доступ в ИСПДн, заводится отдельная учетная запись и выдаются минимально необходимые права для выполнения своих должностных обязанностей.

5.8. В случае временного прекращения выполнения работником обработки персональных данных (отпуск, в том числе декретный, командировка) учетная запись в ИСПДн блокируется, а в случае увольнения сотрудника учетная запись должна удаляться.

5.9. Все изменения в ИСПДн, касающиеся изменения прав доступа сотрудников ФГУП НИИР к обрабатываемым персональным данным, а также изменения особенностей функционирования ИСПДн должны согласовываться с отделом ЗИ ПДТР (а для филиалов с назначенными администраторами безопасности).

VI. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

6.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде

документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

6.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

6.3. При неавтоматизированной обработке персональных данных на бумажных носителях необходимо выполнять следующие требования:

6.3.1. Не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы.

6.3.2. Персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

6.3.3. Документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

6.3.4. Дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

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

6.4.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, наименование предприятия (ФГУП НИИР, филиал ФГУП НИИР-ЛОНИИР и т.п.) и его адрес, фамилию, имя, отчество и адрес работника, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

6.4.2. Типовая форма должна предусматривать поле, в котором работник ФГУП НИИР может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных при необходимости получения письменного согласия на обработку персональных данных.

6.4.3. Типовая форма должна быть составлена таким образом, чтобы со своими персональными данными каждый из работников ФГУП НИИР имел возможность ознакомиться, не нарушая прав и законных интересов других работников.

6.4.4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию ФГУП НИИР, должны соблюдаться следующие условия:

6.5.1. Необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена документом, 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 ФГУП НИИР без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных.

6.5.2. Копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается.

6.5.3. 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 ФГУП НИИР.

6.6. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации. Для электронных носителей персональных данных должны быть разработаны и утверждены генеральным директором ФГУП НИИР (директорами филиалов) правила обращения с ними.

6.7. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные и технические меры, исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

6.8. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6.9. 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).

VII. ТРЕБОВАНИЯ К ОБЕЗЛИЧИВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Обезличивание персональных данных должно обеспечивать защиту от несанкционированного использования и сохранять возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

7.2. К свойствам обезличенных данных относятся:

7.2.1. Полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имела до обезличивания).

7.2.2. Структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания).

7.2.3. Релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме).

7.2.4. Семантическая целостность (сохранение семантики персональных данных при их обезличивании).

7.2.5. Применимость (возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (далее – оператор, операторы), без предварительного деобезличивания всего объема записей о субъектах).

7.2.6. Анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

7.3. В качестве методов обезличивания могут использоваться:

7.3.1. Метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным).

7.3.2. Метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений).

7.3.3. Метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств).

7.3.4. Метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

7.4. При проведении обезличивания следует руководствоваться приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

VIII. ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной, гражданско-правовой и административной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации.

Приложение №1

**СОГЛАСИЕ НА
ОБРАБОТКУ И ПЕРЕДАЧУ
ПЕРСОНАЛЬНЫХ
ДАнных**

_____ дата

_____ Генеральному директору

Должность руководителя организации

_____ ФГУП НИИР

наименование организации

_____ 105064, г. Москва, ул. Казакова, д. 16

_____ В.В. Бутенко

инициалы и фамилия руководителя

от _____

фамилия, имя, отчество работника

_____ Адрес по регистрации

_____ Паспортные данные

Я,

_____ даю согласие на автоматизированную, а также без использования средств автоматизации обработку следующих персональных данных: ФИО, паспортные данные, дата рождения, должность, адрес регистрации, ИНН, номер страхового свидетельства государственного страхования, сведения об образовании, сведения о трудовом стаже в целях соблюдения законодательства, обеспечения личной безопасности, контроля выполняемой работы, обеспечения сохранности имущества.

Перечень действий с персональными данными:

- формирование кадровых документов и выполнения требований Трудового кодекса;
- начисления заработной платы, исчисления и уплаты предусмотренных законодательством налогов, сборов и взносов на обязательное страхование;
- осуществление добровольного страхования от несчастных случаев и страхование здоровья;
- урегулирование страхового случая, имевшего место в результате ДТП на служебном автомобиле;
- бронирование гостиниц и авиабилетов при направлении в командировку;
- оформление ведомственных и государственных наград;
- оформление доверенностей;
- получение лицензий;
- участие в конкурсах;
- представление установленной законодательством отчетности в отношении физических лиц;
- размещение моих фотографий, имени, отчества, должности на внутреннем сайте АС-НИИР;
- предоставление персональных данных по письменному запросу уполномоченных контролирующих органов.

Данное согласие действительно с _____ до даты расторжения трудового договора. Согласие может быть полностью или частично отозвано субъектом персональных данных на основе его заявления.

_____ подпись работника

_____ расшифровка подписи: Ф.И.О.

Приложение № 2

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я, _____,

Ф.И.О.

исполняющий (ая) должностные обязанности по занимаемой должности

должность, наименование структурного подразделения

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение трех лет после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

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

(фамилия, инициалы)

(подпись)

« ____ » _____ Г.
(дата)

Лист согласования

Внутренний документ "проект положения о защите персональных данных"

Должность	Виза	Дата	ФИО	Примечание
Начальник отдела	Согласовано	06.03.2015	Огородничук Александр Дмитриевич	
Начальник отдела	Согласовано	06.03.2015	Каташинская Светлана Вячеславна	
Директор службы	Согласовано	06.03.2015	Кузнецов Сергей Валентинович	
Директор службы	Согласовано	06.03.2015	Тютюнова Вера Анатольевна	
Директор службы	Согласовано	10.03.2015	Цыплаков Сергей Алексеевич	
Главный бухгалтер	Согласовано	25.03.2015	Негляд Валентина Павловна	
Начальник отдела	Согласовано	26.03.2015	Железнякова Анна Юрьевна	
Заместитель генерального директора	Согласовано	26.03.2015	Михайлов Виктор Павлович	