ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»
(ОАО «РЖД»)

РАСПОРЯЖЕНИЕ

«11» июля 2017 г. Москва № 1327р

Об утверждении Инструкции по обработке и защите в ОАО «РЖД» персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных

С целью совершенствования порядка обработки и защиты в ОАО «РЖД» персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных:

1. Утвердить прилагаемую Инструкцию по обработке и защите в ОАО «РЖД» персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных.

2. Руководителям подразделений аппарата управления, филиалов и структурных подразделений ОАО «РЖД»:

а) принять к руководству Инструкцию, утвержденную настоящим распоряжением;

б) ознакомить под подпись с Инструкцией, утвержденной настоящим распоряжением, ответственных за организацию обработки персональных данных и уполномоченных на обработку персональных данных;

в) привести в соответствие с Инструкцией, утвержденной настоящим распоряжением, внутренние организационно-распорядительные документы, регламентирующие порядок обработки и защиты персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных.

3. Начальнику Департамента управления дочерними и зависимыми обществами Кусту С.А. и начальнику Центра по корпоративному управлению пригородным комплексом Белянкину А.Ю.:

а) обеспечить доведение утвержденной настоящим распоряжением Инструкции до дочерних и зависимых обществ ОАО «РЖД»;

б) рекомендовать дочерним и зависимым обществам ОАО «РЖД» привести в соответствие с Инструкцией, утвержденной настоящим распоряжением, нормативные документы, регламентирующие порядок обработки и защиты в дочерних и зависимых обществах ОАО «РЖД»

персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных.

4. Начальнику Управления по защите персональных данных Ерину Л.Т. контролировать исполнение подразделениями аппарата управления, филиалами и структурными подразделениями ОАО «РЖД», а также его дочерними и зависимыми обществами требований утвержденной настоящим распоряжением Инструкции и оказывать им методическую помощь.

5. Контроль за исполнением настоящего распоряжения возложить на вице-президента Федосеева Н.В.

Президент
ОАО «РЖД» О.В.Белозёров

Исп. Мокроусова О.Н., ЦУЗПД
(499) 262-04-85

УТВЕРЖДЕНА
распоряжением ОАО «РЖД»
от «11» 07 2017 г. № 1327р

ИНСТРУКЦИЯ
по обработке и защите в ОАО «РЖД» персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных

I. Общие положения

1. Настоящая Инструкция, разработанная в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687 и «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119, иными нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных, Политикой ОАО «РЖД» по обработке и защите персональных данных (далее – Политика) и другими нормативными документами ОАО «РЖД», определяет основные правила обработки и защиты в ОАО «РЖД» персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных.

2. Требования настоящей Инструкции подлежат исполнению подразделениями аппарата управления, филиалами и структурными подразделениями ОАО «РЖД» (далее – подразделения ОАО «РЖД»), обрабатывающими персональные данные пользователей услуг, контрагентов и иных субъектов персональных данных.

Положения настоящей Инструкции должны учитываться дочерними и зависимыми обществами ОАО «РЖД» при подготовке внутренних нормативных документов по организации обработки и защиты персональных данных.

3. ОАО «РЖД» является оператором, самостоятельно или совместно с другими лицами организующим и (или) осуществляющим обработку персональных данных субъектов персональных данных в целях, определенных в разделе III Политики.

Обработка персональных данных, не отвечающая целям обработки, запрещается.

4. Положения настоящей Инструкции распространяются в том числе на случаи, когда ОАО «РЖД» выступает лицом, осуществляющим обработку персональных данных по поручению стороннего оператора. Дополнительные условия по обработке и защите персональных данных указываются в договоре между ОАО «РЖД» и сторонним оператором.

5. В настоящей Инструкции используются следующие понятия и термины:

1) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

2) автоматизированное рабочее место – рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций;

3) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

4) вымарывание персональных данных – действия, исключающие дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе;

5) допуск к обработке персональных данных – процедура оформления права на доступ к персональным данным;

6) доступ к персональным данным – возможность обработки персональных данных;

7) информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

8) контрагент – юридическое или физическое лицо, с которым ОАО «РЖД» состоит в договорных отношениях или планирует вступить в договорные отношения;

9) материальный носитель – бумажный или машинный носитель информации, предназначенный для фиксирования, передачи и хранения персональных данных;

10) машинный носитель – материальный носитель информации, предназначенный для записи и воспроизведения информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами (внутренние жесткие диски, флэш-накопители, внешние жесткие диски, CD-диски и иные устройства);

11) неавтоматизированная обработка персональных данных – обработка персональных данных, осуществляемая при непосредственном участии человека без использования средств вычислительной техники;

12) несъемный машинный носитель – машинный носитель, встроенный в корпус средства вычислительной техники, используемый для хранения и обработки информации (внутренние жесткие диски и иные устройства);

13) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

14) 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 (в том числе вымарывание), уничтожение персональных данных;

15) ответственный за организацию обработки персональных данных в подразделении ОАО «РЖД» – уполномоченное лицо, назначаемое руководителем подразделения ОАО «РЖД»;

16) передача персональных данных – любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств, представляющих собой доступ, распространение, предоставление персональных данных;

17) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

18) пользователи услуг ОАО «РЖД» – пассажиры, грузоотправители, грузополучатели либо иные физические или юридические лица, пользующиеся услугами, оказываемыми ОАО «РЖД»;

19) смешанная обработка персональных данных – обработка персональных данных, осуществляемая как неавтоматизированным, так и автоматизированным способами;

20) средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

21) субъекты персональных данных – пользователи услуг, контрагенты, а также иные лица, чьи персональные данные стали известны ОАО «РЖД» при осуществлении своей деятельности;

22) съемный машинный носитель – машинный носитель, используемый для хранения информации вне ПЭВМ (флэш-накопители, внешние жесткие диски, CD-диски и иные устройства);

23) трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или юридическому лицу;

24) удаление персональных данных – действия, в результате которых становится невозможным ознакомиться с содержанием персональных данных в информационной системе или на материальном носителе информации;

25) уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе и (или) в результате которых уничтожаются материальные носители персональных данных;

26) уполномоченные работники – работники ОАО «РЖД», имеющие допуск к персональным данным субъектов персональных данных.

II. Правила обработки персональных данных в ОАО «РЖД»

6. Обработка персональных данных субъектов персональных данных в ОАО «РЖД» должна осуществляться с соблюдением законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области обработки и защиты персональных данных.

7. При определении содержания и объема обрабатываемых персональных данных необходимо руководствоваться принципом достаточности по отношению к целям обработки персональных данных при исполнении своих обязательств перед субъектами персональных данных. Состав персональных данных, обрабатываемых в ОАО «РЖД», определен в разделе VI Политики.

8. Допуск и доступ работников ОАО «РЖД» к обработке персональных данных субъектов персональных данных осуществляется в соответствии с Порядком обработки и обеспечения режима защиты персональных данных работников ОАО «РЖД», утвержденным приказом ОАО «РЖД» от 20 июля 2016 г. № 60 (далее – Порядок).

В соответствии с Порядком в подразделениях ОАО «РЖД» и их структурных подразделениях назначаются ответственные за организацию обработки персональных данных и утверждаются списки работников, уполномоченных на обработку персональных данных.

9. Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением следующих случаев:

1) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом;

2) обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на ОАО «РЖД» функций, полномочий и обязанностей, в том числе при перенаправлении обращений граждан, содержащих вопросы, решение которых не входит в компетенцию ОАО «РЖД», в соответствующий орган, организацию или должностному лицу по принадлежности в соответствии с Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»;

3) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

4) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации ОАО «РЖД» своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) обработка персональных данных необходима для осуществления прав и законных интересов ОАО «РЖД» или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

8) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

9) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции и об обязательных видах страхования и в соответствии со страховым законодательством;

10) в иных случаях, предусмотренных законодательством Российской Федерации.

10. Субъект персональных данных вправе отозвать согласие на обработку персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных их обработка может быть продолжена без согласия субъекта персональных данных при наличии оснований, указанных в пункте 9 настоящей Инструкции, и иных оснований, предусмотренных законодательством Российской Федерации.

11. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», запись, систематизация, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан Российской Федерации должны осуществляться с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных федеральными законами.

12. Для фиксации персональных данных, цели обработки которых заведомо несовместимы, используются отдельные материальные носители (бумажные или съемные машинные), отдельные базы данных или файлы на несъемных машинных носителях.

13. При обработке различных категорий персональных данных для каждой категории персональных данных используются отдельные материальные носители (бумажные или съемные машинные), отдельные базы данных или файлы на несъемных машинных носителях.

14. Все машинные носители персональных данных, эксплуатируемые в подразделениях ОАО «РЖД», учитываются в соответствующих журналах учета.

Съемные машинные носители, предназначенные для обработки персональных данных, перед началом их использования учитываются в журнале учета машинных носителей персональных данных, который ведется по форме согласно приложению № 11 к Порядку, которая приведена в приложении № 1 к настоящей Инструкции. В графу 3 журнала вносится учетный номер съемного машинного носителя.

Учетные реквизиты наносятся непосредственно на съемный машинный носитель или на этикетку (бирку, ярлык и т.п.), прикрепленную (наклеенную) на носитель. Учетные реквизиты должны содержать условное или сокращенное наименование подразделения, учетный номер и признак персональных данных (например, 3/ЦДИ/ПДн, 26/ТЧ-2/ПДн).

Несъемные машинные носители персональных данных (внутренние жесткие диски) автоматизированных рабочих мест могут учитываться как в журналах по форме согласно приложению № 1 к настоящей Инструкции, так и в журналах учета несъемных машинных носителей персональных данных, которые ведутся по форме согласно приложению № 2 к настоящей Инструкции.

Несъемные машинные носители персональных данных (внутренние жесткие диски) других средств вычислительной техники (серверов и иных устройств), эксплуатируемые в подразделениях ОАО «РЖД», учитываются в журнале учета несъемных машинных носителей персональных данных, который ведется по форме согласно приложению № 2 к настоящей Инструкции.

В качестве номеров машинных носителей могут использоваться идентификационные (серийные) номера машинных носителей, присвоенные их производителями, номера инвентарного учета, в том числе инвентарные номера технических средств (системного блока, моноблока и т.п.), имеющих встроенные носители информации (внутренние жесткие диски).

Несъемные машинные носители персональных данных, входящие в состав средств вычислительной техники информационных систем, могут учитываться в технических паспортах информационных систем в установленном ОАО «РЖД» порядке. В этом случае в журнале учета несъемных машинных носителей персональных данных учетный номер присваивается всей информационной системе в целом. В графе 2 журнала учета несъемных машинных носителей персональных данных указывается наименование информационной системы, а в графу 3 вносится один учетный номер на все машинные носители, используемые в информационной системе, и указывается номер технического паспорта информационной системы.

15. Сроки обработки (в том числе хранения) персональных данных определяются Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным приказом Минкультуры России от 25 августа 2010 г. № 558, и Перечнем документов, образующихся в деятельности ОАО «РЖД», с указанием сроков хранения, утвержденным распоряжением ОАО «РЖД» от 28 декабря 2007 г. № 2474р, а также целями обработки персональных данных, определенными в разделе III Политики.

16. Персональные данные подлежат уничтожению в следующих случаях и в указанные сроки:

1) по достижению целей обработки – в 30-дневный срок;

2) в случае утраты необходимости достижения целей обработки – в 30-дневный срок;

3) в случае отзыва субъектом персональных данных согласия на обработку персональных данных – в 30-дневный срок, если иной не предусмотрен федеральными законами, договором или соглашением между ОАО «РЖД» и субъектом персональных данных;

4) при выявлении неправомерной обработки персональных данных – в срок, не превышающий 10 рабочих дней с даты выявления.

17. Передача персональных данных субъектов персональных данных без их согласия допускается:

1) третьим лицам с целью предупреждения угрозы жизни и здоровью субъекта персональных данных (например, передача персональных данных в учреждения здравоохранения);

2) в автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже) транспортных средств (АЦБПДП) Министерства транспорта Российской Федерации с целью обеспечения транспортной безопасности;

3) в налоговые органы (например, при направлении ОАО «РЖД» налоговой отчетности);

4) по мотивированному запросу органов прокуратуры, правоохранительных органов и органов безопасности, по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;

5) в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом, по перечню оповещаемых органов и сроков направления извещений о несчастном случае, установленному Трудовым кодексом Российской Федерации.

18. Передача персональных данных в случае, если ОАО «РЖД» поручает их обработку третьим лицам, осуществляется в соответствии с заключенными договорами на оказание услуг и с письменного согласия субъектов персональных данных. Договор должен содержать перечень действий (операций) с персональными данными, цели обработки, обязанность лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии с законодательством Российской Федерации и нормативными документами ОАО «РЖД».

Перед заключением договора с третьими лицами необходимо запросить у них документы либо их надлежащим образом заверенные копии, подтверждающие выполнение условий соблюдения конфиденциальности и обеспечения безопасности персональных данных субъектов персональных данных при их обработке, в том числе:

1) политика (положение, порядок и др.) оператора по обработке и защите персональных данных;

2) акт определения уровня защищенности персональных данных;

3) модель угроз безопасности персональных данных;

4) документы, описывающие состав и содержание мер по обеспечению безопасности персональных данных, аттестаты соответствия требованиям

по безопасности информации для установленного уровня защищенности персональных данных, и другие документы.

19. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, перечень которых утвержден Роскомнадзором, осуществляется в соответствии с Федеральным законом «О персональных данных» и нормативными документами ОАО «РЖД».

20. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, осуществляется в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия субъекта персональных данных в письменной форме.

21. Трансграничная передача как один из способов обработки персональных данных должна соответствовать целям сбора персональных данных. В случае если трансграничная передача персональных данных на территорию государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, не соответствует цели сбора персональных данных, то даже при наличии согласия субъекта персональных данных на такую передачу трансграничная передача персональных данных запрещается.

22. Обработка персональных данных в ОАО «РЖД» может осуществляться автоматизированным, неавтоматизированным и смешанным способами.

В процессе обработки персональных данных допускается многократный переход от неавтоматизированного способа обработки к автоматизированному и наоборот.

III. Неавтоматизированная обработка персональных данных

23. Уполномоченные работники, осуществляющие неавтоматизированную обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, осуществляемой без использования средств вычислительной техники, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных федеральными законами, нормативными правовыми актами органов исполнительной власти Российской Федерации, а также нормативными документами ОАО «РЖД».

24. Персональные данные при их неавтоматизированной обработке обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

25. Персональные данные фиксируются на материальном носителе неавтоматизированным способом (например, записью «от руки» на листе бумаги) или автоматизированным способом (выводом на печать или копированием информации, содержащей персональные данные, на носитель с использованием средств вычислительной техники).

26. Бумажные носители и съемные машинные носители персональных данных хранятся в сейфах, запираемых шкафах или ящиках столов, находящихся в помещениях подразделений ОАО «РЖД». Перечни указанных помещений формируются ответственными за организацию обработки персональных данных и утверждаются соответствующими руководителями подразделений ОАО «РЖД» или их структурных подразделений по форме согласно приложению № 10 к Порядку, которая приведена в приложении № 3 к настоящей Инструкции.

27. Материальные носители, содержащие персональные данные, обрабатываемые в различных целях, хранятся раздельно (в разных шкафах, на разных полках, в отдельных ящиках или папках и т.п.).

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

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, анкеты, карточки, реестры, журналы и др.) должны содержать сведения о цели обработки персональных данных, 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 оператором способов обработки персональных данных. Указанные сведения должны отражаться хотя бы в одном из связанных с типовой формой документов (включая саму типовую форму);

2) типовая форма должна исключать объединение полей, предназначенных для персональных данных, цели обработки которых заведомо не совместимы;

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

4) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных.

29. В случаях, предусмотренных Инструкцией по организации пропускного и внутриобъектового режима в административных зданиях ОАО «РЖД» и на прилегающих территориях, утвержденной приказом ОАО «РЖД» от 16 апреля 2013 г. № 36, ведутся журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территории, на которых находятся подразделения ОАО «РЖД». Для таких журналов (реестров, книг) должны соблюдаться следующие условия:

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

2) 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.

30. Пересылка материальных носителей персональных данных организациям, государственным органам, а также между подразделениями ОАО «РЖД», расположенными по различным адресам, производится в запечатанных конвертах (пакетах) с сопроводительным документом по форме согласно приложению № 4 к настоящей Инструкции, в котором указываются наличие персональных данных и требование о соблюдении конфиденциальности персональных данных.

Пересылка конвертов (пакетов) с материальными носителями, содержащими персональные данные, может производиться фельдъегерской

связью, заказными или ценными почтовыми отправлениями, а также нарочным (работником подразделения ОАО «РЖД» или работником организации-адресата) с распиской о получении документов в реестре.

31. Передача материальных носителей персональных данных между подразделениями ОАО «РЖД» осуществляется уполномоченными работниками в соответствии с запросом или письменным поручением руководителя подразделения ОАО «РЖД» с распиской о получении в реестре или других учетных формах подразделения.

Особенности неавтоматизированной обработки персональных данных, содержащихся на бумажных носителях

32. Подготовка, оформление, прохождение (согласование), регистрация и хранение бумажных носителей персональных данных определяются Инструкцией по делопроизводству и документированию управленческой деятельности в ОАО «РЖД», утвержденной приказом ОАО «РЖД» от 17 июня 2013 г. № 55, и другими нормативными документами ОАО «РЖД» с учетом требований, предусмотренных Политикой.

33. Систематизация обрабатываемых в подразделении ОАО «РЖД» документов, содержащих персональные данные, производится согласно утвержденной в этом подразделении номенклатуре дел.

Разработка номенклатуры дел проводится с учетом требований о раздельном хранении персональных данных, цели обработки которых заведомо несовместимы, и сроков хранения, определяемых пунктом 15 настоящей Инструкции.

34. При ознакомлении субъекта персональных данных со своими персональными данными обеспечивается невозможность его ознакомления с персональными данными иных лиц, содержащимися на тех же бумажных носителях (путем извлечения документов из дела, закрытия чистым листом бумаги и т.п.).

35. При необходимости использования или распространения части персональных данных, находящихся на бумажном носителе, эти персональные данные копируются на другой бумажный носитель.

36. Удаление или обезличивание части персональных данных, если это допускается бумажным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на бумажном носителе (вымарывание).

37. Уточнение персональных данных производится путем обновления или изменения данных на бумажном носителе, а если это не допускается

особенностями бумажного носителя – путем фиксации на том же бумажном носителе сведений о вносимых в них изменениях либо путем изготовления нового бумажного носителя с уточненными персональными данными.

38. Бумажные носители, содержащие персональные данные, включая черновики и промежуточные версии рабочих документов, подлежат уничтожению либо содержащиеся в них персональные данные подлежат обезличиванию по достижении целей обработки или в случае утраты необходимости достижения этих целей, а также по окончании срока их хранения.

Уничтожение производится в соответствии с Инструкцией по делопроизводству и документированию управленческой деятельности в ОАО «РЖД», а также путем сжигания или с помощью устройств для измельчения бумаги (шредеров), не допускающих возможность восстановления исходного документа (шредеры должны быть не ниже уровня секретности 3 (Р-3) – площадь фрагментов не должна превышать 320 мм^2 (например, 4 * 50 мм) или ширина полосы не более 2 мм).

Особенности неавтоматизированной обработки персональных данных, содержащихся на съемных машинных носителях

39. При необходимости использования или распространения части персональных данных, находящихся на съемном машинном носителе, эти персональные данные копируются на другой съемный машинный носитель, учтенный согласно пункту 14 настоящей Инструкции.

40. Персональные данные, записанные на съемные машинные носители, удаляются в соответствии с требованиями третьего абзаца пункта 50 настоящей Инструкции.

41. Съемные машинные носители, не допускающие возможности удаления персональных данных, уничтожаются путем физического разрушения машинного носителя, не позволяющего произвести последующее считывание или восстановление записанных на машинном носителе персональных данных, в установленном ОАО «РЖД» порядке. В журнале учета машинных носителей персональных данных производится соответствующая запись об уничтожении, заверенная подписями уполномоченного работника и лица, осуществляющего учет машинных носителей подразделения.

IV. Автоматизированная обработка персональных данных

42. Автоматизированная обработка персональных данных производится с помощью средств вычислительной техники, как установленных локально, так и объединенных в информационные системы.

43. Доступ к информационным системам, обрабатывающим персональные данные, предоставляется уполномоченным работникам в рамках функций, предусмотренных их должностными инструкциями, и осуществляется в соответствии с Порядком предоставления доступа к информационным системам ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от 28 ноября 2011 г. № 2546р.

В случае, когда ОАО «РЖД» выступает в качестве лица, осуществляющего обработку персональных данных по поручению оператора, доступ к информационным системам оператора осуществляется на основании договора между ОАО «РЖД» и оператором.

44. При автоматизированной обработке персональные данные содержатся на машинных носителях персональных данных.

Фиксация персональных данных на машинном носителе производится с использованием средств вычислительной техники (копирование персональных данных на любой съемный или несъемный машинный носитель, ввод персональных данных в базу данных и т.п.).

45. Уточнение персональных данных производится путем обновления или изменения данных на машинном носителе с помощью средств вычислительной техники. Если это не допускается особенностями машинного носителя, то уточнение производится путем изготовления нового машинного носителя с уточненными персональными данными.

46. Обезличивание персональных данных, обрабатываемых в информационных системах ОАО «РЖД», в случае необходимости осуществляется с учетом Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, утвержденных приказом Роскомнадзора от 5 сентября 2013 г. № 996.

47. При выявлении по обращению субъекта персональных данных либо Роскомнадзора неточных персональных данных в информационной системе ОАО «РЖД» организуется блокирование таких персональных данных на период проверки. В течение 7 рабочих дней со дня подтверждения факта неточности персональные данные уточняются в соответствии с пунктом 45 настоящей Инструкции и разблокируются.

48. При выявлении по обращению субъекта персональных данных либо Роскомнадзора неправомерной обработки персональных данных в информационной системе ОАО «РЖД» организуется блокирование таких персональных данных на период расследования. Расследование проводится в соответствии с разделом VIII Порядка.

В течение 3 рабочих дней с момента выявления неправомерной обработки персональных данных такая обработка прекращается. В случае если

обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных, такие персональные данные уничтожаются.

49. Об устранении допущенных нарушений или об уничтожении (невозможности уничтожения) персональных данных письменно уведомляется автор обращения (субъект персональных данных либо Роскомнадзор) по форме согласно приложению № 9 к Порядку, которая приведена в приложении № 5 к настоящей Инструкции.

50. Удаление персональных данных в информационных системах ОАО «РЖД» производится в соответствии с процедурами, определенными в эксплуатационной документации на информационные системы, обрабатывающие персональные данные.

Удаление персональных данных на отдельных средствах вычислительной техники (рабочих местах уполномоченных работников) производится штатными средствами информационных и (или) операционных систем.

Удаление части персональных данных на съемном машинном носителе, если это допускает носитель, производится с использованием штатных средств информационных и (или) операционных систем с сохранением возможности обработки иных данных, зафиксированных на машинном носителе.

51. Копирование информации с одного съемного машинного носителя персональных данных на другой и уничтожение персональных данных на съемном машинном носителе производятся только на средствах вычислительной техники, предназначенных для обработки персональных данных.

52. При отправке средств вычислительной техники, предназначенных для обработки персональных данных, для проведения гарантийных и ремонтных работ машинные носители персональных данных из них предварительно удаляются.

53. Если ремонту подлежат машинные носители, содержащие персональные данные, имеющаяся на них информация гарантированно уничтожается в установленном ОАО «РЖД» порядке. Если гарантированное уничтожение информации на машинных носителях персональных данных невозможно, то такие машинные носители ремонту не подлежат и должны быть физически уничтожены в соответствии с требованиями пункта 54 настоящей Инструкции.

54. Пришедшие в негодность или отслужившие установленный срок машинные носители персональных данных уничтожаются путем физического разрушения машинного носителя, не позволяющего произвести последующее считывание или восстановление записанных на машинном носителе персональных данных, в установленном ОАО «РЖД» порядке.

Уничтожение несъемных машинных носителей персональных данных производится по акту в установленном для средств вычислительной техники порядке.

Уничтожение съемных машинных носителей персональных данных может производиться без оформления акта.

В журналах учета машинных носителей персональных данных производится соответствующая запись об их уничтожении.

V. Рассмотрение обращений (запросов) субъектов персональных данных

55. Субъекты персональных данных имеют право получать информацию, касающуюся обработки их персональных данных в ОАО «РЖД», в соответствии с частями 1 – 7 статьи 14 Федерального закона «О персональных данных».

56. При получении обращения (запроса) от субъекта персональных данных ему (или его представителю) предоставляются сведения, касающиеся обработки его персональных данных в ОАО «РЖД».

Сведения предоставляются в доступной форме, в них не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Ответы на письменные запросы граждан и организаций даются в письменной форме.

57. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Федерального закона «О персональных данных» все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Запрос должен содержать данные основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись (в том числе электронная) субъекта персональных данных или его представителя.

58. При получении повторного запроса от субъекта персональных данных ранее, чем через 30 дней после первоначального обращения (запроса), и предоставлении ему сведений в полном объеме по результатам рассмотрения

первоначального обращения (запроса) ОАО «РЖД» вправе отказать субъекту персональных данных в выполнении повторного запроса.

59. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных» в том случае, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

VI. Обеспечение безопасности персональных данных при их обработке

60. Обеспечение безопасности персональных данных при их обработке в ОАО «РЖД» осуществляется в соответствии:

1) с законодательством Российской Федерации в области обработки и защиты персональных данных;

2) с требованиями ФСТЭК России, ФСБ России и Роскомнадзора;

3) с нормативными документами ОАО «РЖД».

61. Комплекс мер, обеспечивающих безопасность персональных данных, включает в себя в том числе:

1) организацию работы с персональными данными, обеспечивающей сохранность носителей персональных данных и средств защиты информации;

2) размещение информационных систем, обрабатывающих персональные данные, и специального оборудования в помещениях, исключающих возможность неконтролируемого пребывания в них посторонних лиц;

3) разграничение доступа пользователей и работников, обслуживающих средства вычислительной техники, к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

4) учет документов и информационных массивов, содержащих персональные данные;

5) регистрацию действий пользователей информационных систем, обрабатывающих персональные данные, и работников, обслуживающих средства вычислительной техники в установленном ОАО «РЖД» порядке;

6) контроль действий и недопущение несанкционированного доступа к персональным данным пользователей информационных систем ОАО «РЖД» и персонала, обслуживающего средства вычислительной техники;

7) хранение и использование материальных носителей персональных данных, исключающих их хищение, подмену и уничтожение;

8) необходимое резервирование технических средств и дублирование массивов и носителей информации, содержащей персональные данные.

62. Для каждой информационной системы, обрабатывающей персональные данные, в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, в зависимости от уровня защищенности персональных данных при их обработке в информационных системах назначается должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе, либо на одно из структурных подразделений ОАО «РЖД» возлагаются функции по обеспечению безопасности персональных данных в информационной системе.

63. Организационные и (или) технические меры защиты для каждой информационной системы, обрабатывающей персональные данные, определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе ОАО «РЖД».

Уровень защищенности информационных систем, обрабатывающих персональные данные, определяется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Методическими указаниями по классификации АСУ ОАО «РЖД» для задания требований защиты информации в соответствии с Приказом ФСТЭК от 18 февраля 2013 г. № 21, утвержденными ОАО «РЖД» 21 сентября 2015 г.

64. Обработка персональных данных осуществляется уполномоченными работниками с обязательным принятием мер, исключающих возможность ознакомления с персональными данными посторонних лиц, в том числе работников ОАО «РЖД», не уполномоченных на обработку персональных данных, таких как:

1) экран монитора размещается таким образом, чтобы исключить возможность просмотра информации посторонними лицами (в том числе другими работниками подразделения);

2) уполномоченные работники используют для доступа к информационным системам, обрабатывающим персональные данные, индивидуальные пароли, отвечающие установленным в ОАО «РЖД» требованиям;

3) средства вычислительной техники блокируются с помощью защищенной паролем экранной заставки во время перерывов в работе;

4) в информационных системах, обрабатывающих персональные данные, и (или) на отдельных автоматизированных рабочих местах, предназначенных

для работы с персональными данными, в обязательном порядке используются средства антивирусной защиты. При отсутствии таких средств или окончании срока действия лицензии на них подается соответствующая заявка в Единую службу поддержки пользователей;

5) все пароли доступа работника ОАО «РЖД» к информационным системам, обрабатывающим персональные данные, в обязательном порядке меняются при его переходе из одного подразделения ОАО «РЖД» в другое;

6) бумажные носители, содержащие персональные данные, размещаются таким образом, чтобы исключить возможность просмотра информации посторонними лицами (в том числе другими работниками подразделения);

7) все бумажные или съемные машинные носители с персональными данными помещаются в сейфы, запираемые шкафы или ящики столов после окончания работы с ними либо при оставлении рабочего помещения;

8) испорченные бланки, черновики и промежуточные редакции документов, содержащие персональные данные, по окончании работы с ними уничтожаются в соответствии с Инструкцией по делопроизводству и документированию управленческой деятельности в ОАО «РЖД».

65. При работе с персональными данными уполномоченным работникам запрещается:

1) работать под чужими или общими учетными записями в информационных системах, обрабатывающих персональные данные, и передавать кому-либо индивидуальные пароли;

2) допускать использование своего автоматизированного рабочего места другими работниками ОАО «РЖД» и посторонними лицами;

3) использовать (загружать, запускать и т.п.) для обработки персональных данных программные средства, не разрешенные для применения в информационных системах ОАО «РЖД»;

4) сообщать ставшие им известными в связи с исполнением своих должностных обязанностей персональные данные лицам, не имеющим права доступа к этим данным;

5) делать копии документов, содержащих персональные данные, не требующиеся для выполнения своих служебных обязанностей;

6) держать на рабочем месте материальные носители с персональными данными дольше времени, необходимого на их обработку.

66. Работник ОАО «РЖД» немедленно ставит в известность руководителя своего подразделения:

1) о факте утраты (утери, хищения) материальных носителей персональных данных;

2) о факте разглашения или неправомерной обработки персональных данных;

3) о ставших известными ему фактах или возможностях несанкционированного доступа к информационным системам, обрабатывающим персональные данные.

Приложение № 1
к Инструкции по обработке и защите
в ОАО «РЖД» персональных данных
пользователей услуг, контрагентов и
иных субъектов персональных данных

ЖУРНАЛ
учета машинных носителей персональных данных

№ п/п	Вид машинного носителя	Номер машинного носителя	Дата постановки на учет машинного носителя	Ф.И.О., должность работника, получившего машинный носитель в пользование	Дата и подпись работника в получении машинного носителя	Дата возврата и подпись уполномоченного работника в получении машинного носителя от работника	Дата и подпись уполномоченного работника и исполнителя об уничтожении машинного носителя
1	2	3	4	5	6	7	8

Образец учетных реквизитов
(наносится на машинный носитель)

Условное или сокращенное наименование подразделения
Учетный номер

Приложение № 2
к Инструкции по обработке и защите
в ОАО «РЖД» персональных данных
пользователей услуг, контрагентов и
иных субъектов персональных данных

ЖУРНАЛ
учета несъемных машинных носителей персональных данных

№ п/п	Наименование ИС, вид машинного носителя, его местонахождение (номер помещения)	Номер машинного носителя/номер техпаспорта на ИС	Дата постановки на учет	Сокращенное наименование подразделения, должность, фамилия и инициалы работника, эксплуатирующего машинный носитель	Дата и подпись работника, эксплуатирующего машинный носитель	Дата возврата или окончания эксплуатации машинного носителя и подпись работника, ведущего учет	Отметка об уничтожении машинного носителя (номер и дата акта)
1	2	3	4	5	6	7	8

Приложение № 3
к Инструкции по обработке и защите
в ОАО «РЖД»персональных данных
пользователей услуг, контрагентов и
иных субъектов персональных данных

УТВЕРЖДАЮ

_____
(должность руководителя подразделения ОАО «РЖД»)

_____ _____
(подпись) (Ф.И.О.)
«___» _____ 20___ г.

ПЕРЕЧЕНЬ

помещений_____,
(наименование подразделения ОАО «РЖД»)

в которых хранятся материальные носители персональных данных

№ п/п	Номер помещения	Адрес (место расположения)

Приложение № 4
к Инструкции по обработке и защите
в ОАО «РЖД»персональных данных
пользователей услуг, контрагентов и
иных субъектов персональных данных

Руководителю

_____
(Ф.И.О. руководителя)
«____» _____ 20___ г.

Уважаемый(ая) _____!

В ответ на Ваш запрос (письмо, обращение) от _____ № _____, сообщаю, что _____
_____
_____.

Предоставленная Вам информация относится к персональным данным и в соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» является конфиденциальной.

Указанные персональные данные могут быть использованы Вами исключительно в целях, указанных в Вашем запросе (письме, обращении) от _____ № _____.

_____ / _____ / _____
(должность) (подпись) (расшифровка подписи)

«____» _____ 20___ г.

Приложение № 5
к Инструкции по обработке и защите
в ОАО «РЖД» персональных данных
пользователей услуг, контрагентов и
иных субъектов персональных данных

УВЕДОМЛЕНИЕ
об устранении нарушений обработки или уничтожении (невозможности уничтожения) персональных данных

Уважаемый(ая)_____!
(Ф.И.О.)

Настоящим уведомляем, что Ваше обращение от_____
(дата обращения,
_____
краткое содержание обращения)
_____
_____
_____рассмотрено.

Выявленное(ые) нарушение(я) обработки Ваших персональных данных:_____
(краткое описание нарушения)
_____
_____
(устранены, уничтожены/уничтожение невозможно по причине)
_____.

_____/_____/_____
(должность) (подпись) (расшифровка подписи)

«___» _____ 20___ г.

Уведомление
получил: _____/_____
(подпись субъекта персональных данных) (расшифровка подписи)

«___» _____ 20___ г.