УТВЕРЖДЕНО  
приказом Росжелдора  
от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_

**Правила обработки и обеспечения защиты персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта**

1. **Общие положения**
   1. Настоящие Правила обработки и обеспечения защиты персональных данных (далее – Правила) в центральном аппарате Федерального агентства железнодорожного транспорта (далее – Росжелдор) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области правил обработки и защиты персональных данных, (далее - ПДн), а также определяют 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. Целью настоящего документа является формирование общих правил для обеспечения защиты ПДн, обрабатываемых в государственных информационных системах Росжелдора, от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.
   3. Правила разработаны в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом Российской Федерации от 27 июля 2006 г. № 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» и иными нормативными правовыми актами в области обеспечения защиты ПДн, действующими на территории Российской Федерации.
   4. В настоящем документе используются следующие термины:

* персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
* оператор (в данном случае Росжелдор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
* обработка персональных данных – любое действие (операция) или совокупность действий (операций), 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;
* автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
* неавтоматизированная обработка персональных данных – обработка персональных данных субъекта без использования средств вычислительной техники;
* распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
* предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
* блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
* уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
* обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
* информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
* трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
* безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе;
* контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;
* конфиденциальность персональных данных – обязательное для соблюдения оператором или иным лицом, получившим доступ к персональным данным, требования не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.
* технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1. **Область действия**
   1. Правила являются обязательными для исполнения всеми государственными гражданскими служащими Росжелдора, осуществляющими обработку персональных данных и имеющих доступ к ним.
2. **Обработка персональных данных субъектов персональных данных**
   1. Государственные гражданские служащие Росжелдора не имеют права получать и обрабатывать персональные данные субъектов, не соответствующие целям их обработки.
   2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются государственными гражданскими служащими Росжелдора.
   3. Передавать персональные данные субъектов для обработки третьим лицам можно только после получения Росжелдором от субъекта персональных данных письменного согласия на передачу конкретному лицу (организации), кроме случаев, установленных действующим законодательством Российской Федерации. Передача персональных данных на материальном носителе информации фиксируется в соответствующих журналах работниками, ответственными за документооборот в Росжелдоре. Передача персональных данных в электронном виде по защищенным каналам связи фиксируется в электронных журналах средств защиты информации.
   4. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:
      1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
      2. фамилию, имя, отчество, адрес представителя субъекта персональных данных, 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 персональных данных);
      3. наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
      4. цель обработки персональных данных;
      5. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
      6. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
      7. перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
      8. срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
      9. подпись субъекта персональных данных.
   5. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных или в случае достижения целей обработки персональных данных государственный гражданский служащий Росжелдора, ответственный за организацию обработки и обеспечение безопасности персональных данных инициирует сбор, блокировку обработки с последующим уничтожением персональных данных субъекта, кроме случаев, установленных законодательством Российской Федерации.
   6. При обработке персональных данных субъекта по его запросу могут быть предоставлены следующие данные:

* подтверждение факта обработки персональных данных в Росжелдоре;
* правовые основания и цели обработки персональных данных;
* применяемые в Росжелдоре способы обработки персональных данных;
* наименование и место нахождения Росжелдора, сведения о лицах (за исключением работников Росжелдора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Росжелдором или на основании Федерального закона;
* обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
* сроки обработки персональных данных, в том числе сроки их хранения;
* порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
* наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Росжелдора, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные федеральными законами.
  1. В случае получения запросов от уполномоченного органа по защите прав субъектов персональных данных в адрес Росжелдора работник, ответственный за организацию обработки и обеспечение безопасности персональных данных, обязан представить документы и локальные акты по обеспечению безопасности обработки персональных данных субъектов и (или) иным образом подтвердить принятие необходимых мер в течение тридцати дней с даты получения такого запроса.
  2. В соответствии с законодательством Российской Федерации в целях обеспечения прав и свобод человека и гражданина Росжелдор при обработке персональных данных субъекта должны соблюдать следующие общие требования:
* обработка персональных данных должна осуществляться на законной и справедливой основе;
* обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
* не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
* обработке подлежат только персональные данные, которые отвечают целям их обработки;
* содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
* 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. Росжелдор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
* хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
* при определении объема и содержания обрабатываемых персональных данных Росжелдор должен руководствоваться действующим законодательством Российской Федерации и локальными нормативными актами Росжелдора;
* при принятии решений, затрагивающих интересы субъекта, Росжелдор не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;
* защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Росжелдором в порядке, установленном действующим законодательством Российской Федерации;
* государственные гражданские служащие Росжелдора должны быть ознакомлены под роспись с организационно-распорядительными документами Росжелдора, устанавливающими порядок обработки и защиты персональных данных, а также об их правах и обязанностях в этой области;
* доступ государственных гражданских служащих Росжелдора к персональным данным субъектов персональных данных в информационных системах регламентируется только на основании локальных нормативных актов Росжелдора с указанием перечня допущенных лиц, прав доступа, необходимых для выполнения служебных обязанностей;
* 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;
* 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);
* 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;
* при хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.
  1. При передаче персональных данных субъекта государственными гражданскими служащими Росжелдора должны соблюдаться следующие требования:
* не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Федеральным законом;
* осуществлять передачу персональных данных субъектов в пределах Росжелдора в соответствии с нормативными документами внутреннего документооборота.
  1. Допускается передача персональных данных субъектов сторонним организациям, если данная передача обусловлена Федеральным законом либо соответствующим соглашением и не нарушает прав субъекта персональных данных.
  2. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Росжелдор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Росжелдор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.
  3. В случае подтверждения факта неточности персональных данных Росжелдор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.
  4. В случае выявления неправомерной обработки персональных данных, осуществляемой Росжелдором или лицом, действующим по поручению Росжелдора, Росжелдор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Росжелдора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Росжелдор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Росжелдор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
  5. В случае достижения цели обработки персональных данных Росжелдор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.
  6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Росжелдор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) 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 персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ или другими федеральными законами.
  7. В случае отсутствия возможности уничтожения персональных данных в течение установленного срока, Росжелдор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.
  8. Государственные гражданские служащие Росжелдора несут персональную ответственность за сохранность персональных данных, к которым они имеют доступ.
  9. Государственные гражданские служащие Росжелдора, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к ответственности, предусмотренной действующим законодательством Российской Федерации и локальными нормативными актами Росжелдора.

1. **Оценка угроз безопасности информации**
   1. Материальными носителями персональных данных, применяющимися в технических средствах и системах, являются: бумажные носители и накопители на жестких магнитных дисках.
   2. Основные виды угроз и источники угроз безопасности представлены в частных моделях угроз безопасности для каждой государственной информационной системы Росжелдора.
2. **Цели и сроки обработки данных в информационных системах персональных данных**
   1. Цели и сроки хранения данных в государственных информационных системах персональных данных Росжелдора определяются в рамках каждой государственной информационной системы персональных данных отдельно в соответствующей модели угроз, утверждаемой в установленном порядке, с обязательным указанием нормативных документов, регламентирующих сроки хранения. Основным документом, регламентирующим сроки хранения, является Федеральный закон Российской Федерации от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации».
3. **Организационные мероприятия по защите персональных данных при их обработке в государственных информационных системах персональных данных Росжелдора**
   1. Организационные мероприятия по защите персональных данных связаны с формированием пакета документов по защите персональных данных, их разработкой, официальным оформлением и доведением до исполнителей, а также организацией контроля за соблюдением установленных этими документами правил и требований. Состав внутренних документов, разрабатываемых на основании действующего законодательства Российской Федерации и локальных нормативных актов Росжелдора, определяется на этапе приведения процессов обработки персональных данных в Росжелдора в соответствие требованиям законодательства. Состав документов определяется Росжелдором при возможном привлечении организаций-лицензиатов.
   2. Мероприятия должны исключить возможность утечки информации, обрабатываемой в государственных информационных системах персональных данных Росжелдора, и обеспечить запрет передачи персональных данных по открытым каналам связи без применения установленных мер по ее защите, а также исключить возможность внесения в контролируемую зону устройств регистрации и накопления информации без соответствующего разрешения.
   3. Обязанность поддерживать комплект документов по защите персональных данных в актуальном состоянии возлагается на ответственного за организацию обработки и обеспечение безопасности персональных данных.
   4. Организационные мероприятия по защите персональных данных, обрабатываемых на автоматизированных рабочих местах государственных гражданских служащих Росжелдора, должны быть связаны с обеспечением:

* ограничения физического доступа и контроля доступа к техническим средствам, обрабатывающим персональные данные;
* сохранности съемных и машинных носителей информации, материалов печати и исключения доступа к ним посторонних лиц;
* исключения возможностей несанкционированного просмотра изображений с монитора автоматизированного рабочего места через дверные проемы, окна – в том числе с использованием средств телевизионной, фотографической и визуальной оптической разведки, находящихся за границами контролируемой зоны;
* режима блокирования доступа к автоматизированному рабочему месту во время отсутствия государственного гражданского служащего на месте;
* режима блокирования доступа в помещение с установленным автоматизированным рабочим местом в рабочее время при отсутствии государственного гражданского служащего на месте.
  1. Организационные мероприятия по защите персональных данных в локальных вычислительных сетях Росжелдора должны осуществлять:
* обеспечение режима запрета на вхождение в локально вычислительную сеть под чужой учетной записью;
* обеспечение периодической смены паролей пользователями;
* обеспечение хранения файлов с информацией в групповых каталогах (каталогах, информация в которых является доступной для определенной группы лиц), структура которых однозначно отображает организационную структуру управления/отдела, и разрешения доступа к нему только государственных гражданских служащих соответствующей структурной единицы;
* обеспечение файлового обмена информацией между пользователями управления/отдела через создаваемый каталог общего использования, информация в котором является доступной для имеющих санкционированный доступ в локально-вычислительной сети пользователей;
* обеспечение контроля присвоения пользователям учетных записей и их удаление или блокирование при увольнении государственного гражданского служащего Росжелдора;
* обеспечение резервного копирования электронных информационных ресурсов;
* обеспечение режима разграничения и контроля доступа к аппаратным и программным ресурсам локальных вычислительных сетей и автоматизированных рабочих мест.

1. **Технические мероприятия по защите персональных данных**
   1. Технические мероприятия по защите информации разрабатываются по результатам обследования автоматизированных государственных информационных систем персональных данных, предназначенных для обработки персональных данных, и оценки возможностей обеспечения защиты на основе применения организационных мер защиты и активизации встроенных механизмов защиты используемых операционных систем и аппаратного обеспечения.
   2. Требуется осуществлять следующие технические мероприятия:

* применение сертифицированных средств антивирусной защиты;
* применение сертифицированных программных и (или) аппаратных средств защиты информации от несанкционированного доступа, контроля целостности, регистрации и учета действий пользователей государственных информационных систем персональных данных Росжелдора;
* защита персональных данных при межсетевом взаимодействии с использованием сертифицированных средств защиты;
* применение сертифицированных средств для организации защищенного канала для передачи персональных данных по каналам связи;
* предотвращение несанкционированной записи персональных данных на съемные носители информации или вывода персональных данных на печать;
* регулярный мониторинг и контроль защищенности системы защиты информации.

1. **Контроль состояния системы защиты персональных данных**
   1. В рамках проверок состояния защиты персональных данных рекомендуется осуществлять контроль:

* наличия в управлениях нормативных документов по защите информации и доведения их до государственных гражданских служащих под роспись;
* знания и выполнения государственными гражданскими служащими требований локальных нормативных актов Росжелдора по защите персональных данных при их обработке в государственных информационных системах Росжелдора;
* наличия и комплектности эксплуатационной и технической документации на систему защиты информации, а также факта ознакомления государственных гражданских служащих Росжелдора и работников подведомственных и подрядных организаций с инструкциями пользователя и администратора государственной информационной системы, а также инструкцией администратора информационной безопасности с соответствующей отметкой об ознакомлении в инструкциях;
* работоспособности системы защиты информации;
* определение (актуализация) требований по безопасности персональных данных при разработке (модернизации) государственных информационных систем персональных данных Росжелдора.
  1. Контроль за состоянием системы защиты персональных данных осуществляется в плановом и внеплановом порядке ответственным за организацию обработки и обеспечение безопасности персональных данных, назначаемым руководителем Росжелдора.

1. **План контрольных мероприятий**
   1. С целью выявления и предотвращения нарушений законодательства Российской Федерации в сфере защиты персональных данных, ответственными за организацию обработки и обеспечение безопасности персональных данных проводятся контролирующие мероприятия в соответствии с планом мероприятий по обеспечению защиты персональных данных.
   2. При возникновении внештатных ситуаций, повлекших несанкционированное уничтожение данных, нарушение целостности и другие несанкционированные изменения информации, проводятся внеплановые контролирующие мероприятия.