

УТВЕРЖДЕНО

приказом АО «ФПК»

от «13» 04 2018 г. № 208

ПОЛОЖЕНИЕ

об обработке и защите персональных данных в АО «ФПК»

І. Общие положения

1. Настоящее Положение об обработке и защите персональных данных в АО «ФПК» (далее – Положение), разработанное в соответствии с законодательством Российской Федерации и локальными нормативными актами АО «ФПК», определяет цели, принципы, условия и правила обработки персональных данных, меры по обеспечению режима их защиты, права и обязанности субъектов персональных данных, а также права, обязанности и ответственность лиц, осуществляющих обработку персональных данных.

2. Настоящее Положение распространяется на аппарат управления АО «ФПК», структурные подразделения АО «ФПК», филиалы АО «ФПК» и их структурные подразделения.

3. АО «ФПК» является оператором, самостоятельно или совместно с другими лицами организующим и (или) осуществляющим обработку персональных данных работников и других субъектов персональных данных в целях:

- обеспечения соблюдения законодательства Российской Федерации;
- обеспечения выполнения трудовых договоров с работниками;
- содействия работникам в обучении и продвижении по службе;
- обеспечения личной безопасности работников;
- исполнения договоров перевозки и предоставления дополнительных услуг во время осуществления перевозки;
- повышения качества обслуживания пассажиров и доступности железнодорожных перевозок путем реализации дополнительных программ поощрения пользователей услуг АО «ФПК»;
- обеспечения транспортной безопасности;
- обеспечения пропуска субъектов персональных данных на объекты АО «ФПК»;
- исполнения обязательств перед физическими лицами, состоящими в договорных и иных гражданско-правовых отношениях с АО «ФПК»;
- проведения маркетинговых исследований, осуществления рекламно-информационных рассылок;

выполнения социальных обязательств, а также в других целях, предусмотренных Уставом АО «ФПК» и локальными нормативными актами АО «ФПК».

4. Настоящее Положение распространяется, в том числе, на случаи, когда АО «ФПК» обрабатывает персональные данные по поручению стороннего оператора. Дополнительные условия по обработке и защите персональных данных указываются в договоре между АО «ФПК» и сторонним оператором.

5. Действие настоящего Положения не распространяется на отношения, возникающие:

при хранении, комплектовании, учете и использовании сведений, содержащих персональные данные, архивных документов АО «ФПК» (документов, законченных делопроизводством и переданных на хранение в соответствующий архив АО «ФПК») в соответствии с законодательством об архивном деле в Российской Федерации;

при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

6. Работники АО «ФПК» несут персональную ответственность за обеспечение режима защиты персональных данных, выполнение работниками требований законодательства Российской Федерации и нормативных документов АО «ФПК» в области обработки и защиты персональных данных.

II. Термины, сокращения и условные обозначения

7. В настоящем Положении используются следующие термины, сокращения и условные обозначения:

автоматизированная обработка персональных данных – обработка персональных данных, при которой такие действия с персональными данными, как уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются без непосредственного участия человека;

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;

биометрические персональные данные – сведения, характеризующие физиологические и биологические особенности субъекта персональных данных, которые используются оператором для установления личности субъекта персональных данных;

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

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

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

защита персональных данных – деятельность АО «ФПК», включающая принятие правовых, организационных и технических мер, направленных на обеспечение защиты от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;

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

контрагент – юридическое или физическое лицо, с которым АО «ФПК» состоит в договорных отношениях или планирует вступить в договорные отношения;

контролируемая зона – пространство (административные здания АО «ФПК», прилегающая к ним территория), на котором на законных основаниях осуществляется контроль за пребыванием и действиями физических лиц и (или) транспортных средств;

конфиденциальность персональных данных – обязательное для соблюдения АО «ФПК» требование не раскрывать третьим лицам персональные данные и не допускать их распространения без согласия субъектов персональных данных или наличия иного законного основания;

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

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

неавтоматизированная обработка персональных данных – обработка персональных данных, при которой такие действия с персональными данными, как уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при

непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации (автоматизированной) только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее;

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

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

ответственный за организацию обработки персональных данных в подразделении АО «ФПК» – начальник подразделения АО «ФПК»;

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;

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

подразделения – подразделения аппарата управления, структурные подразделения АО «ФПК», филиалы АО «ФПК» и их структурные подразделения;

пользователи услуг АО «ФПК» – пассажиры и иные физические или юридические лица, пользующиеся услугами, оказываемыми АО «ФПК»;

ПЭВМ – персональная электронная вычислительная машина;

работник – физическое лицо, вступившее в трудовые отношения с АО «ФПК»;

разглашение персональных данных – действия (бездействие), в результате которых персональные данные в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без письменного согласия субъекта персональных данных;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

режим защиты персональных данных – нормативно установленные правила, определяющие ограничения доступа к персональным данным, порядок передачи и условия их хранения;

СНИ – съемные машинные носители информации, используемые для хранения информации вне ПЭВМ (флеш-накопители, внешние жесткие диски, CD и иные устройства);

специальные категории персональных данных – персональные данные субъектов персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни и судимости;

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

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

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

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

уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах АО «ФПК».

III. Состав и категории персональных данных, обрабатываемых в АО «ФПК»

8. Категории персональных данных, обрабатываемых в АО «ФПК»:

персональные данные, обрабатываемые в АО «ФПК» в соответствии с законодательством Российской Федерации и локальными нормативными актами АО «ФПК» с учетом целей обработки персональных данных, указанных в пункте 3 настоящего Положения;

специальные категории персональных данных, касающиеся состояния здоровья работников (в соответствии с требованиями федеральных законов от

27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»);

данные о судимости (в соответствии с требованиями Федерального закона от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»);

биометрические персональные данные (в соответствии с требованиями Федерального закона № 152-ФЗ).

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (корпоративные справочники, адресные книги и прочее), в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных, могут включаться:

фамилия, имя, отчество;

место работы;

занимаемая должность;

номера стационарных и мобильных рабочих телефонов;

адреса корпоративной электронной почты;

фотография работника.

9. Состав персональных данных, обрабатываемых в АО «ФПК»:

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

число, месяц, год рождения;

место рождения;

сведения о гражданстве (подданстве), в том числе предыдущие гражданства, иные гражданства;

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

адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

номера рабочих, домашних и мобильных телефонов или сведения о других способах связи;

реквизиты свидетельства обязательного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты полиса обязательного медицинского страхования;

реквизиты свидетельства о браке;

сведения о семейном положении, составе семьи и близких родственниках, обрабатываемые в соответствии с законодательством Российской Федерации;

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация);

сведения об ученой степени;

сведения о владении иностранными языками, включая уровень владения;

фотография работника;

сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору;

сведения о пребывании за границей;

сведения о наличии или отсутствии судимости – только кандидатов для приема на работу (соискателей) – в случаях, определенных федеральными законами;

сведения об оформленных допусках к государственной тайне;

сведения о государственных наградах, иных наградах и знаках отличия;

сведения о профессиональной переподготовке и (или) повышении квалификации;

результаты медицинского обследования работника на предмет годности к выполнению трудовых обязанностей;

сведения о ежегодных оплачиваемых отпусках, отпусках работников, совмещающих работу с обучением (учебных отпусках), и отпусках без сохранения заработной платы;

сведения о заработной плате, реквизиты банковского счета для перечисления заработной платы и социальных выплат;

пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный);

дата поездки;

пол;

дата и место рождения;

контактный телефон;

адрес электронной почты;

полный почтовый адрес (в случае участия в Программе лояльности «РЖД Бонус» холдинга «РЖД»);

гражданство;

другие персональные данные, необходимые для обеспечения реализации целей обработки, указанных в пункте 3 настоящего Положения.

IV. Принципы, условия и правила обработки персональных данных в АО «ФПК»

10. Принципы обработки персональных данных:

1) обработка персональных данных должна осуществляться на законной и справедливой основе;

2) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных;

3) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;

4) обработке подлежат только те персональные данные, которые отвечают целям их обработки;

5) доступ к персональным данным разрешается только работникам, которым эти персональные данные необходимы для исполнения должностных обязанностей;

6) 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;

7) при определении содержания и объема обрабатываемых персональных данных и предоставлении доступа к ним необходимо руководствоваться принципом минимальной достаточности по отношению к целям обработки персональных данных при исполнении своих обязательств перед субъектами персональных данных;

8) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

11. Условия обработки персональных данных:

1) обработка персональных данных с согласия субъектов персональных данных, если иное не предусмотрено законодательством Российской Федерации;

2) выполнение возложенных на АО «ФПК» законодательством Российской Федерации и Уставом АО «ФПК» функций, полномочий и обязанностей;

3) осуществление правосудия, исполнения судебных актов, актов других органов и должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

4) исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также заключение договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5) защита жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия невозможно;

6) осуществление прав и законных интересов оператора или третьих лиц либо достижение общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) опубликование или обязательное раскрытие информации в соответствии с законодательством Российской Федерации.

12. 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 11 настоящего Положения, и иных оснований, предусмотренных законодательством Российской Федерации.

13. Персональные данные обрабатываются в АО «ФПК» следующими способами:

неавтоматизированная обработка;

автоматизированная обработка.

14. Работники должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством Российской Федерации, а также локальными нормативными актами АО «ФПК».

15. При сборе персональных данных, в том числе посредством сети Интернет, обработка персональных данных граждан Российской Федерации должна осуществляться с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных законодательством Российской Федерации.

16. Для обработки персональных данных, цели обработки которых заведомо несовместимы, используются отдельные материальные носители (бумажные или съемные машинные), отдельные базы данных или файлы на несъемных машинных носителях. Материальные носители, содержащие персональные данные, обрабатываемые в различных целях, хранятся отдельно (в разных шкафах, на разных полках, в отдельных ящиках или папках и т.п.).

17. 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.

18. АО «ФПК» вправе поручить с согласия субъекта персональных данных обработку персональных данных другому лицу на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации в области обработки и защиты персональных данных и настоящим Положением.

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

20. Передача персональных данных третьим лицам, в том числе трансграничная передача, допускается только с письменного согласия субъектов персональных данных, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью субъектов персональных данных, а также в иных случаях, предусмотренных законодательством Российской Федерации.

21. Персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

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

4) в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом, по перечню оповещаемых органов и с соблюдением сроков направления извещений о несчастном случае, установленных Трудовым кодексом Российской Федерации;

5) в иных случаях, предусмотренных законодательством Российской Федерации.

V. Меры по обеспечению режима защиты персональных данных

23. Безопасность персональных данных обеспечивается реализацией комплекса мер, определенных законодательством Российской Федерации, нормативными документами АО «ФПК», в том числе включающих:

- 1) определение угроз безопасности персональных данных при их обработке;
- 2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- 3) проведение проверки соответствия применяемых мер защиты информации и оценки их эффективности законодательству Российской Федерации в области обработки и защиты персональных данных;
- 4) обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер;
- 5) восстановление персональных данных, измененных или уничтоженных вследствие несанкционированного доступа к ним;
- 6) установление правил доступа к персональным данным, обрабатываемым в информационной системе, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе АО «ФПК», в установленном АО «ФПК» порядке;
- 7) внутренний контроль за соблюдением подразделениями АО «ФПК» при обработке персональных данных законодательства Российской Федерации и нормативных документов АО «ФПК»;
- 8) размещение информационных систем АО «ФПК» и специального оборудования в помещениях, исключающих возможность неконтролируемого пребывания в них посторонних лиц;
- 9) разграничение доступа пользователей и работников, обслуживающих средства вычислительной техники, к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- 10) учет машинных носителей, информационных массивов, содержащих персональные данные;
- 11) регистрацию действий пользователей информационных систем и работников, обслуживающих средства вычислительной техники, в установленном в АО «ФПК» порядке;
- 12) контроль действий и недопущение несанкционированного доступа к персональным данным пользователей информационных систем АО «ФПК», персонала, обслуживающего средства вычислительной техники;
- 13) хранение и использование материальных носителей, исключаящие их

хищение, подмену и уничтожение;

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

24. Осуществление внутреннего контроля соблюдения законодательства Российской Федерации и нормативных документов АО «ФПК» при обработке персональных данных подразделениями осуществляется на основании предписания о проведении проверки за подписью заместителя Генерального директора, возглавляющего блок безопасности.

25. Для каждой информационной системы, обрабатывающей персональные данные, в соответствии с законодательством Российской Федерации в зависимости от уровня защищенности персональных данных при их обработке в информационных системах назначается работник, ответственный за обеспечение безопасности персональных данных в информационной системе.

26. Меры защиты персональных данных при их автоматизированной обработке устанавливаются в соответствии со специальными требованиями к технической защите информации, определенными Федеральной службой по техническому и экспортному контролю (ФСТЭК России), а также в соответствии с локальными нормативными актами АО «ФПК» в области обеспечения информационной безопасности.

27. При автоматизированной обработке персональных данных для каждой информационной системы организационные и (или) технические меры определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе АО «ФПК».

28. При работе с персональными данными 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 АО «ФПК» и посторонними лицами;

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

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 исполнения своих должностных обязанностей;

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

29. Работник АО «ФПК» немедленно информирует непосредственного руководителя:

- 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.

VI. Права и обязанности субъектов персональных данных

30. Субъекты персональных данных имеют право:

- 1) на получение по запросу полной информации о своих персональных данных, обрабатываемых подразделениями АО «ФПК»;
- 2) на получение по запросу копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;
- 3) на уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- 4) на дополнение своих персональных данных заявлением, выражающим собственную точку зрения;
- 5) на извещение всех лиц, которым ранее были сообщены их неверные или неполные персональные данные, обо всех произведенных в них исправлениях или дополнениях;
- 6) на отзыв согласия на обработку своих персональных данных;
- 7) на обжалование в соответствии с законодательством Российской Федерации действий АО «ФПК» при обработке персональных данных или его бездействия;
- 8) на осуществление иных прав, предусмотренных законодательством Российской Федерации.

31. Субъекты персональных данных обязаны:

- 1) предоставлять АО «ФПК» свои персональные данные в соответствии с законодательством Российской Федерации и настоящим Положением;
- 2) своевременно информировать АО «ФПК» об изменениях своих персональных данных;
- 3) обеспечивать конфиденциальность персональных данных других субъектов персональных данных в соответствии с требованиями законодательства Российской Федерации, Кодекса деловой этики и других нормативных документов АО «ФПК».

VII. Обязанности АО «ФПК»

32. АО «ФПК» обязано принимать следующие необходимые и достаточные меры для исполнения обязанностей оператора, предусмотренных законодательством Российской Федерации:

1) назначать ответственных за организацию обработки персональных данных;

2) издавать документы, определяющие политику АО «ФПК» в отношении обработки персональных данных, нормативные документы по вопросам обработки персональных данных, а также нормативные документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и устранение последствий таких нарушений;

3) применять правовые, организационные и технические меры для защиты персональных данных субъектов персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;

4) разъяснять субъектам персональных данных юридические последствия отказа предоставить их персональные данные, если предоставление персональных данных является обязательным в соответствии с законодательством Российской Федерации;

5) блокировать неправомерно обрабатываемые персональные данные, прекращать обработку персональных данных в соответствии с законодательством Российской Федерации;

6) уведомлять субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных;

7) представлять субъектам персональных данных по их запросу или их представителям информацию, касающуюся обработки их персональных данных, в порядке, установленном законодательством Российской Федерации и локальными нормативными актами АО «ФПК». 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.);

8) осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных законодательству Российской Федерации и локальным нормативным актам АО «ФПК»;

9) проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации;

Федерации о персональных данных, соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области обработки и защиты персональных данных.

VIII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

33. Лица, виновные в нарушении законодательства Российской Федерации и требований локальных нормативных актов АО «ФПК» в области обработки и защиты персональных данных, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность.

34. Ущерб, причиненный субъектам персональных данных вследствие нарушения их прав, правил обработки персональных данных, а также требований к защите персональных данных, установленных законодательством Российской Федерации и локальными нормативными актами АО «ФПК» в области обработки и защиты персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации.

IX. Допуск к обработке персональных данных

35. Основанием для допуска работника к обработке персональных данных являются должностная инструкция, предусматривающая обработку персональных данных, обязательство о неразглашении персональных данных, составленное по форме согласно приложению № 1 к настоящему Положению, подписанное работником.

36. Доступ к информационным системам, обрабатывающим персональные данные, предоставляется работникам в рамках функций, предусмотренных их должностными инструкциями, и осуществляется в соответствии с локальными нормативными актами АО «ФПК» и по согласованию с Управлением корпоративной безопасности (работниками, ответственными за корпоративную безопасность в филиалах).

37. Начальник подразделения обеспечивает:

ознакомление под роспись уполномоченных работников с настоящим Положением;

подписание уполномоченными работниками обязательства о неразглашении персональных данных, составленного по форме согласно приложению № 1 к настоящему Положению. Обязательство о неразглашении персональных данных хранится в личном деле работника.

Х. Требования к обработке персональных данных

38. Требования к обработке персональных данных распространяются на персональные данные, состав и категории которых определены в разделе III настоящего Положения.

39. При приеме на работу у субъекта персональных данных берется согласие на обработку его персональных данных, в том числе на включение персональных данных в общедоступные источники персональных данных (корпоративные справочники, адресные книги), которое оформляется в соответствии с приложением № 2 к настоящему Положению.

40. В случаях, предусмотренных законодательством Российской Федерации, когда обработка персональных данных субъекта персональных данных осуществляется только с его согласия, оператор получает у субъекта персональных данных согласие на обработку его персональных данных, составленное по форме согласно приложению № 3 к настоящему Положению.

41. Согласие на обработку персональных данных должно быть получено у субъекта персональных данных до начала их обработки.

42. Документы, подтверждающие согласие на обработку персональных данных работников, хранятся в их личных делах.

43. Получение согласия близких родственников работника на обработку их персональных данных не требуется при заполнении анкет в объеме, предусмотренном унифицированной формой № Т-2, либо в случаях, установленных законодательством Российской Федерации (исполнение законодательства в сфере транспортной безопасности, получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат и другие случаи).

44. В иных случаях получение согласия близких родственников работника является обязательным условием обработки их персональных данных и оформляется в соответствии с приложением № 3 к настоящему Положению.

45. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть проинформирован об этом заранее путем направления ему уведомления по форме согласно приложению № 4 к настоящему Положению и дать письменное согласие на получение персональных данных у третьих лиц, составленное по форме согласно приложению № 5 к настоящему Положению.

АО «ФПК» сообщает работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о составе подлежащих получению персональных данных и последствиях отказа работника от дачи письменного согласия на их получение.

Необходимость согласия на получение персональных данных у третьих лиц и направления уведомления об этом может возникнуть, например, при подтверждении факта получения диплома, свидетельства, аттестата об образовании, при восстановлении трудовой книжки, свидетельства о получении квалификации, при подтверждении факта работы на предыдущем месте, факта смены фамилии и др., в том числе если утрата сведений произошла в связи со стихийными бедствиями, иными обстоятельствами.

46. АО «ФПК» не вправе запрашивать у третьих лиц даже с согласия субъекта персональных данных информацию, не имеющую отношения к целям обработки персональных данных.

47. Если при обращении субъекта персональных данных либо уполномоченного органа по защите прав субъектов персональных данных выявлены неточные персональные данные или неправомерная обработка персональных данных, АО «ФПК» обязано осуществить блокирование таких персональных данных до их актуализации.

При подтверждении факта неточности персональных данных АО «ФПК» обязано уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

При выявлении неправомерной обработки персональных данных АО «ФПК» обязано прекратить их обработку в срок, не превышающий трех рабочих дней с даты выявления. В случае если обеспечить правомерность обработки персональных данных невозможно, АО «ФПК» обязано уничтожить такие персональные данные в срок, не превышающий десять рабочих дней с даты выявления неправомерной обработки персональных данных.

48. Об устранении допущенных нарушений или об уничтожении персональных данных (невозможности уничтожить их в срок, установленный Федеральным законом № 152) АО «ФПК» обязано письменно информировать субъекта персональных данных путем уведомления по форме согласно приложению № 6 к настоящему Положению и приобщить копию уведомления или справку об уведомлении к материалам расследования (проверки).

49. При обработке персональных данных кандидатов, поступающих на работу, оформляется согласие в соответствии с приложением № 3 к настоящему Положению.

При этом предусмотрены следующие исключения:

1) письменное согласие не требуется, если от имени кандидата действует кадровое агентство, с которым он заключил соответствующий договор, а также при самостоятельном размещении кандидатом своего резюме в сети Интернет, доступного неограниченному кругу лиц;

2) письменное согласие кандидата не требуется при поступлении резюме кандидата из банка вакансий, размещенных на сайте АО «ФПК», так как

согласие заполняется при размещении резюме на сайте;

3) если резюме кандидата поступило по электронной почте или факсу, уполномоченному работнику необходимо подтвердить факт направления указанного резюме самим кандидатом. Если из резюме невозможно однозначно определить физическое лицо, его направившее, данное резюме подлежит уничтожению в день поступления.

50. Обезличивание персональных данных, обрабатываемых в информационных системах АО «ФПК», в случае необходимости осуществляется с учетом Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утвержденных приказом Роскомнадзора от 5 сентября 2013 г. № 996.

51. Сроки хранения, комплектования, учета, передачи и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов регламентируются Федеральным законом от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», 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, Инструкцией по делопроизводству и документированию управленческой деятельности в акционерном обществе «Федеральная пассажирская компания».

52. Для каждой информационной системы АО «ФПК» организационные и (или) технические меры определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе.

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

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

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется

копирование персональных данных, подлежащих распространению или использованию;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию.

55. При использовании типовых форм документов, в которые предполагается или допускается включение персональных данных, должны соблюдаться условия, предусмотренные Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в контролируемую зону или в иных аналогичных целях, должны соблюдаться условия, предусмотренные Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

56. Уточнение персональных данных производится путем их обновления или изменения на материальном носителе, а если это не допускается особенностями материального носителя – путем изготовления нового материального носителя с уточненными персональными данными.

57. При работе с документами, содержащими персональные данные, должны быть приняты меры, исключающие возможность нарушения их конфиденциальности.

58. Средства защиты информации, обеспечивающие защиту персональных данных, должны удовлетворять Требованиям к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, а также нормативным правовым актам в области обработки и защиты персональных данных ФСТЭК России и Федеральной службы безопасности (ФСБ России).

59. Автоматизированная обработка персональных данных разрешается только при условии применения средств защиты информации, обеспечивающих нейтрализацию актуальных угроз, определенных Федеральным законом № 152-ФЗ.

60. Во время эксплуатации средств вычислительной техники, предназначенных для обработки персональных данных, должны быть предусмотрены меры по исключению случаев несанкционированного

подключения к внешним информационным системам, внешним информационно-телекоммуникационным сетям, а также несанкционированного доступа к этим средствам при проведении ремонтных, профилактических и других видов работ.

61. Во время перерывов в работе, а также после окончания работы с документами, содержащими персональные данные, необходимо:

1) убирать документы с поверхности рабочих столов в запирающееся хранилище (сейф, шкаф);

2) блокировать средство вычислительной техники с помощью защищенной паролем экранной заставки;

3) принимать необходимые меры по недопущению использования средства вычислительной техники другими работниками и посторонними лицами.

XI. Требования к обращению с материальными носителями персональных данных, их учету и хранению

62. Персональные данные субъектов персональных данных хранятся на бумажных носителях в соответствии с номенклатурой дел и в электронном виде (в информационных системах АО «ФПК», на ПЭВМ, а также на машинных носителях) с соблюдением условий, обеспечивающих их защиту от несанкционированного доступа.

63. Хранение материальных носителей должно осуществляться в помещениях, находящихся в контролируемой зоне с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

64. В подразделениях, осуществляющих обработку персональных данных с использованием машинных носителей, ведется их учет в журнале, составленном по форме согласно приложению № 7 к настоящему Положению.

На все находящиеся в обращении СНИ, содержащие персональные данные, наносятся учетные реквизиты (непосредственно на СНИ или на прикрепленную (наклеенную) этикетку (бирку, ярлык и т.п.). Учетные реквизиты должны содержать условное или сокращенное наименование подразделения, учетный номер и признак персональных данных (например, 3/ФПКБЗ/ПДн, 26/ФПКФБЗ-МОСК/ПДн).

В качестве серийных номеров машинных носителей могут использоваться идентификационные номера, 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).

65. Выносить машинные носители, содержащие персональные данные, из рабочих помещений без служебной необходимости запрещается.

ХII. Уничтожение персональных данных и их материальных носителей

66. Подразделения АО «ФПК» осуществляют систематический мониторинг персональных данных, цели обработки которых достигнуты или сроки хранения которых истекли, с последующим уничтожением документов, иных материальных носителей, содержащих персональные данные, а также удалением персональных данных, содержащихся в информационных системах АО «ФПК», файлах, хранящихся на ПЭВМ или на внешних перезаписываемых СНИ, в соответствии с законодательством Российской Федерации или при наступлении иных законных оснований.

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

1) по достижении целей обработки или в случае утраты необходимости в достижении целей персональных данных – в 30-дневный срок;

2) в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных – в 30-дневный срок, если иной срок не предусмотрен договором или соглашением между АО «ФПК» и субъектом персональных данных либо если АО «ФПК» не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами;

3) при выявлении неправомерной обработки персональных данных – в срок, не превышающий 7 рабочих дней с даты выявления, в следующих случаях:

а) персональные данные являются неполными, устаревшими, неточными (при условии, что уточнение персональных данных невозможно);

б) персональные данные получены незаконно;

в) персональные данные не являются необходимыми для заявленной цели обработки.

68. В процессе уничтожения дел и документов необходимо исключить возможность ознакомления третьих лиц с содержащимися в них персональными данными.

69. Уничтожение не вошедших в дела документов (копий документов, черновиков), содержащих персональные данные, должно производиться в подразделении АО «ФПК» таким образом, чтобы была исключена возможность прочтения текста уничтоженного документа.

70. Уничтожение персональных данных, хранящихся на ПЭВМ и (или) на перезаписываемых СНИ, производится с использованием штатных средств информационных и операционных систем.

71. В случае использования непerezаписываемых СНИ их уничтожение производится путем механического нарушения целостности, не позволяющего произвести считывание или восстановление содержания персональных данных (надлом, физическое деформирование). В журнале учета СНИ персональных данных производится соответствующая запись об уничтожении, заверенная подписями исполнителя и ответственного работника подразделения АО «ФПК», который осуществляет регистрацию СНИ.

72. Уничтожение или обезличивание части персональных данных, если это допускает материальный носитель, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

73. При утрате или несанкционированном уничтожении СНИ проводится служебное расследование и составляется акт. Соответствующие отметки делаются в журнале учета машинных носителей персональных данных.

ХIII. Передача персональных данных

74. Передача персональных данных субъектов персональных данных без их согласия допускается, если это необходимо для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве, по мотивированным запросам правоохранительных органов и иных органов государственной власти в рамках установленных полномочий, а также в иных случаях, предусмотренных законодательством Российской Федерации.

75. Передача персональных данных субъектов персональных данных третьим лицам осуществляется с их письменного согласия, составленного по форме согласно приложению № 8 к настоящему Положению, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъектов персональных данных, а также в иных случаях, предусмотренных законодательством Российской Федерации.

76. Пересылка материальных носителей, содержащих персональные данные, между различными почтовыми адресами, производится в запечатанных конвертах (пакетах) с сопроводительным документом, в котором сообщается о наличии персональных данных и требованиях о соблюдении конфиденциальности персональных данных.

77. Пересылка конвертов (пакетов) с документами, содержащими персональные данные, может производиться фельдьегерской связью, заказными или ценными почтовыми отправлениями. Допускается передача документов, содержащих персональные данные, нарочным (работником подразделения АО «ФПК» или работником организации-адресата) с распиской о получении документов в реестре.

78. Передача персональных данных между подразделениями АО «ФПК» осуществляется исключительно в служебных целях.

79. Передача персональных данных в электронном виде может осуществляться с использованием только корпоративной почты АО «ФПК» (домен @fpc.ru, @fpc.org.rzd).

При этом передача персональных данных по электронной почте иным операторам (юридическим лицам, органам государственной власти и т.д.) может осуществляться только на адреса, находящиеся в домене последних, и на основании имеющихся договорных отношений, мотивированного запроса или в иных случаях, установленных законодательством Российской Федерации.

80. Размещение персональных данных на сетевых ресурсах АО «ФПК» возможно при соблюдении мер по недопущению ознакомления с ними лиц, не имеющих допуска к обработке таких персональных данных.

81. Запрещено передавать персональные данные с использованием сторонних интернет-сервисов (мессенджеры, социальные сети, облачные хранилища и т.д.) без согласования с Управлением корпоративной безопасности.

82. При необходимости регистрации в Единой автоматизированной системе документооборота АО «ФПК» документа, содержащего персональные данные, создается и регистрируется карточка сопроводительного документа (входящего, исходящего, организационно-распорядительного) или поручения в соответствии с требованиями к оформлению документов по делопроизводству в АО «ФПК». При этом карточке присваивается атрибут «Ограниченный доступ».

83. Пересылка материальных носителей, непосредственная их передача сторонним адресатам осуществляется только с письменного указания руководителя подразделения АО «ФПК», осуществляющего отправку документа.

84. Трансграничная передача персональных данных субъектов 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 уполномоченным органом

по защите прав субъектов персональных данных, осуществляется в соответствии с законодательством Российской Федерации и локальными нормативными актами АО «ФПК».

85. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случае:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных, составленного по форме согласно приложению № 9;

2) соблюдения условий, предусмотренных международными договорами Российской Федерации;

3) выполнения требований федеральных законов, 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.

86. Трансграничная передача персональных данных субъектов персональных данных может быть запрещена или ограничена в целях защиты законных интересов АО «ФПК» и прав субъектов персональных данных.

XIV. Рассмотрение обращений субъектов персональных данных

87. Субъекты персональных данных имеют право получать информацию, касающуюся обработки их персональных данных в АО «ФПК», в соответствии с законодательством Российской Федерации.

88. Сведения предоставляются субъекту персональных данных 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.

89. Сведения в отношении субъекта персональных данных предоставляются по его запросу или запросу его законного представителя.

90. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его

органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с АО «ФПК» (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных АО «ФПК», подпись субъекта персональных данных или его представителя.

Запрос может быть также направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае если в запросе субъекта персональных данных не отражены указанные сведения, то ему направляется мотивированный отказ.

91. В случае если запрашиваемые сведения были предоставлены для ознакомления субъекту персональных данных по его запросу, он вправе обратиться повторно в АО «ФПК» или направить повторный запрос в целях получения этих сведений и ознакомления с ними не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

До истечения этого срока субъект персональных данных вправе обратиться повторно в АО «ФПК» или направить повторный запрос в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

92. АО «ФПК» вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктом 90 настоящего Положения. Такой отказ должен быть мотивированным.

93. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в случаях, установленных законодательством Российской Федерации.

XV. Проведение служебного расследования по фактам разглашения или неправомерной обработки персональных данных

94. В случае выявления фактов разглашения или неправомерной обработки персональных данных в подразделении АО «ФПК» должны быть осуществлены действия, направленные на обеспечение законных прав и свобод субъектов персональных данных, а также приняты исчерпывающие меры по локализации условий, повлекших нарушение режима защиты персональных данных, и минимизации ущерба.

95. О фактах утраты материальных носителей, разглашения персональных данных либо неправомерной обработки персональных данных

информируется письменно ответственный за организацию обработки персональных данных подразделения АО «ФПК», в котором допущено нарушение, а также Управление корпоративной безопасности.

96. Расследование обстоятельств утраты материальных носителей, разглашения либо неправомерной обработки персональных данных проводится с участием представителей подразделения корпоративной безопасности и ответственного за организацию обработки персональных данных в подразделении.

97. При проведении служебного расследования обстоятельств утраты материальных носителей, разглашения либо неправомерной обработки персональных данных:

1) определяется обоснованность отнесения разглашенной либо утраченной информации к персональным данным;

2) устанавливаются обстоятельства и лица, допустившие утрату материальных носителей, разглашение либо неправомерную обработку персональных данных (время, место, способ);

3) принимаются меры к определению местонахождения материальных носителей;

4) оценивается причиненный или возможный вред субъекту персональных данных вследствие утраты материальных носителей, разглашения либо неправомерной обработки персональных данных;

5) составляется заключение о результатах проведенного служебного расследования.

98. Служебное расследование проводится в возможно короткие сроки (не более двадцати календарных дней) со дня установления факта утраты материальных носителей, разглашения либо неправомерной обработки персональных данных.

99. Работники, проводящие служебное расследование, имеют право:

1) опрашивать работников подразделений АО «ФПК», которые допустили утрату материальных носителей, разглашение либо неправомерную обработку персональных данных, а также работников подразделений АО «ФПК», которые могут оказать содействие в установлении обстоятельств допущенного нарушения или в определении местонахождения утраченных материальных носителей, и получать от них письменные объяснения;

2) запрашивать и получать информацию и документы, имеющие отношение к проведению служебного расследования обстоятельств утраты материальных носителей, разглашения либо неправомерной обработки персональных данных;

3) проводить осмотр помещений, в которых хранятся и обрабатываются