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

РАСПОРЯЖЕНИЕ

2 декабря 2019 г. Москва № 2719/р

Об утверждении Положения о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД»

С целью совершенствования контроля за соблюдением режима защиты персональных данных в ОАО «РЖД»:

1. Утвердить прилагаемое Положение о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД» (далее – Положение).

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

организовать изучение Положения ответственными за организацию обработки персональных данных, ответственными за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД» и уполномоченными на обработку персональных данных;

обеспечить исполнение требований Положения при осуществлении внутреннего контроля за соблюдением режима защиты персональных данных.

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

обеспечить доведение Положения до сведения дочерних и зависимых обществ ОАО «РЖД»;

рекомендовать дочерним и зависимым обществам ОАО «РЖД» разработать (привести в соответствие с Положением) нормативные документы, регламентирующие организацию контроля за соблюдением режима защиты персональных данных в дочерних и зависимых обществах ОАО «РЖД».

4. Начальнику Управления по защите персональных данных Шемякину В.В. обеспечить контроль за исполнением требований Положения подразделениями аппарата управления, филиалами и структурными

подразделениями ОАО «РЖД», а также дочерними и зависимыми обществами ОАО «РЖД» и оказывать им методическую помощь.

5. Признать утратившим силу распоряжение ОАО «РЖД» от 12 октября 2016 г. № 2085р «О контроле за соблюдением режима защиты персональных данных в ОАО «РЖД».

6. Контроль за исполнением настоящего распоряжения возложить на заместителя генерального директора ОАО «РЖД» Федосеева Н.В.

Генеральный директор –
председатель правления ОАО «РЖД» О.В.Белозёров

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

УТВЕРЖДЕНО
распоряжением ОАО «РЖД»
от 02.12. 2019 г. № 2719/р

ПОЛОЖЕНИЕ
о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД»

I. Общие положения

1. Настоящее Положение, разработанное в соответствии с федеральными законами «О персональных данных» и «Об информации, информационных технологиях и о защите информации», политикой ОАО «РЖД» по обработке и защите персональных данных, иными нормативными правовыми актами Российской Федерации и нормативными документами ОАО «РЖД», определяет цель, задачи и порядок контроля за соблюдением режима защиты персональных данных в подразделениях аппарата управления, филиалах и структурных подразделениях ОАО «РЖД», а также в региональных (структурных) подразделениях филиалов и структурных подразделений ОАО «РЖД», расположенных в границах железных дорог (далее – подразделения ОАО «РЖД»).

2. В настоящем Положении используются следующие понятия:

1) защита персональных данных – деятельность ОАО «РЖД», включающая принятие правовых, организационных и технических мер, направленных на обеспечение защиты от неправомерных действий в отношении персональных данных;

2) инцидент, связанный с нарушением режима защиты персональных данных, – одно или ряд нежелательных или непредвиденных событий, которые могут нарушить режим защиты персональных данных;

3) контроль за соблюдением режима защиты персональных данных – совокупность действий и операций по мониторингу и проверке соблюдения требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области персональных данных;

4) мониторинг соблюдения режима защиты персональных данных – постоянное наблюдение за процессами обработки и обеспечения безопасности персональных данных, включая рассмотрение поступающей (выявляемой) информации о рисках, связанных с нарушениями режима защиты персональных данных, а также сбор, анализ и обобщение результатов наблюдения.

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

6) режим защиты персональных данных – нормативно установленные правила, определяющие ограничение доступа к персональным данным и процессам их обработки, а также порядок их передачи и условия хранения;

7) риск, связанный с нарушением режима защиты персональных данных, – потенциальная опасность нанесения ущерба ОАО «РЖД» финансового и/или репутационного характера в результате нарушения требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области персональных данных;

3. Целью контроля за соблюдением режима защиты персональных данных (далее – контроль) является оценка в рамках риск-ориентированного подхода соответствия обработки и обеспечения безопасности персональных данных требованиям законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области персональных данных.

4. Задачи контроля:

1) анализ выполнения требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области обработки и обеспечения безопасности персональных данных;

2) выявление рисков, связанных с нарушениями режима защиты персональных данных, установление причин их возникновения;

3) разработка мероприятий по воздействию на выявленные риски для их минимизации (устранения), а также предотвращения их повторного возникновения и реализации.

5. Контроль за соблюдением режима защиты персональных данных и обеспечением их безопасности осуществляется в подразделениях ОАО «РЖД» Управлением по защите персональных данных (далее – Управление), ответственными за организацию обработки персональных данных в подразделениях ОАО «РЖД» и ответственными за обеспечение безопасности персональных данных в информационных системах по кругу ведения.

6. Контроль за выполнением Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, организуют не реже 1 раза в 3 года Управление и ответственные за обеспечение безопасности персональных данных в информационных системах как самостоятельно, так и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7. Координацию деятельности ответственных за организацию обработки персональных данных в подразделениях аппарата управления, филиалах, структурных подразделениях ОАО «РЖД», ответственных за обеспечение безопасности персональных данных в информационных системах и комитетов по организации обработки и обеспечению безопасности персональных данных при региональных оперативных комиссиях железных дорог осуществляет Управление.

8. Координацию деятельности ответственных за организацию обработки персональных данных в региональных (структурных) подразделениях филиалов и структурных подразделений ОАО «РЖД», расположенных в границах железных дорог, осуществляют ответственные за организацию обработки персональных данных соответствующих филиалов и структурных подразделений ОАО «РЖД» и комитеты по организации обработки и обеспечению безопасности персональных данных при региональных оперативных комиссиях железных дорог.

9. При проведении проверок соблюдения законодательства Российской Федерации в области персональных данных контрольно-надзорными органами государственной власти (Роскомнадзором, ФСТЭК России, ФСБ России, органами прокуратуры) руководителям подразделений ОАО «РЖД» необходимо руководствоваться Положением о порядке действия подразделений ОАО «РЖД» при проведении проверок органами, уполномоченными на осуществление государственного контроля (надзора) и муниципального контроля, при исполнении и обжаловании актов и предписаний этих органов и устранении причин, послуживших основанием для привлечения ОАО «РЖД» к административной ответственности, утвержденным распоряжением ОАО «РЖД» от 9 марта 2016 г. № 375р, а также Положением об организации работы по защите интересов ОАО «РЖД» при проведении централизованных проверок ОАО «РЖД» органами, уполномоченными осуществлять государственный контроль (надзор), утвержденным приказом ОАО «РЖД» от 11 января 2018 г. № 2.

10. При получении уведомления контрольно-надзорного органа государственной власти о планируемой (внеплановой) проверке соблюдения законодательства Российской Федерации в области персональных данных, руководитель подразделения ОАО «РЖД» или ответственный за организацию обработки персональных данных в подразделении ОАО «РЖД» в течение 24 часов направляет в Управление копию уведомления, а после завершения проверки – копию акта проверки с соответствующим предписанием (при наличии).

11. Руководитель подразделения ОАО «РЖД» или ответственный за организацию обработки персональных данных в подразделении ОАО «РЖД»

незамедлительно уведомляет Управление о фактах привлечения должностных лиц ОАО «РЖД» или ОАО «РЖД» к административной ответственности за нарушения законодательства Российской Федерации в области персональных данных.

II. Мониторинг соблюдения режима защиты персональных данных

12. Управление осуществляет мониторинг соблюдения режима защиты персональных данных (далее – мониторинг) всех процессов обработки и обеспечения безопасности персональных данных в подразделениях ОАО «РЖД», включая своевременность назначения руководителями подразделений ОАО «РЖД» ответственных за организацию обработки персональных данных в подразделениях ОАО «РЖД» и ответственных за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД».

13. Управление вправе осуществлять мониторинг без взаимодействия с подразделениями ОАО «РЖД».

14. Ответственный за организацию обработки персональных данных в подразделении ОАО «РЖД» по кругу ведения осуществляет мониторинг в части:

1) соблюдения порядка организации доступа к персональным данным;

2) соблюдения требований конфиденциальности при обработке персональных данных;

3) своевременности назначения и установления обязанностей ответственных за организацию обработки персональных данных и ответственных за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД», для которых подразделение является функциональным заказчиком;

4) актуальности списков работников, уполномоченных на обработку персональных данных;

5) включения обязанностей уполномоченных на обработку персональных данных в их должностные инструкции;

6) ознакомления под роспись работников, уполномоченных на обработку персональных данных, с нормативными документами ОАО «РЖД» в области персональных данных;

7) наличия письменных обязательств о неразглашении персональных данных от работников, уполномоченных на обработку персональных данных;

8) актуальности перечней помещений, в которых хранятся материальные носители персональных данных;

9) учета машинных носителей персональных данных;

10) актуальности сведений, содержащихся в паспорте оператора персональных данных подразделения ОАО «РЖД» и его соответствия форме, утвержденной распоряжением ОАО «РЖД» от 25 апреля 2018 г. № 816/р;

11) организации работы с обращениями субъектов персональных данных, их представителей и юридических лиц по вопросам обработки персональных данных.

15. Ответственный за обеспечение безопасности персональных данных в информационной системе ОАО «РЖД» осуществляет мониторинг правомерности доступа к ней работников подразделений ОАО «РЖД» и сторонних организаций, а также мониторинг своевременности проведения классификации информационной системы и оценки эффективности реализованных мер по обеспечению безопасности обрабатываемых в ней персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

16. Ответственный за обеспечение безопасности персональных данных в информационной системе ОАО «РЖД» незамедлительно информирует руководителя подразделения (функционального заказчика) и Управление об утечке персональных данных субъектов персональных данных, которая может серьезно отразиться на правах и основных свободах субъектов персональных данных.

17. По согласованию с ответственным за организацию обработки персональных данных в ОАО «РЖД» для проведения мониторинга информационных систем ОАО «РЖД» могут использоваться специальные программно-технические средства сбора, записи и хранения событий информационной безопасности с возможностью их анализа и уведомления об их возникновении.

18. По факту выявленных в процессе мониторинга рисков, связанных с нарушениями режима защиты персональных данных и обеспечения их безопасности, принимаются меры по их минимизации (устранению), в том числе работы по приведению информационной системы обработки персональных данных в соответствие с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

При необходимости проводится внеплановая проверка соблюдения режима защиты персональных данных.

III. Организация и проведение проверок соблюдения режима защиты персональных данных

19. Проверки соблюдения режима защиты персональных данных (далее также – проверки) организуют Управление и ответственные за организацию обработки персональных данных в подразделениях ОАО «РЖД».

20. Для проведения проверок и контроля процедур, в том числе связанных с автоматизированной обработкой персональных данных, оценки причиненного (возможного) материального и (или) иного вреда субъекту персональных данных, а также ущерба коммерческим интересам ОАО «РЖД» и минимизации имиджевых рисков в соответствии с установленным в ОАО «РЖД» порядке могут привлекаться подразделения ОАО «РЖД», дочерние и зависимые общества ОАО «РЖД» с учетом специфики их деятельности, а также на договорной основе юридические лица и индивидуальные предприниматели.

21. Юридические лица и индивидуальные предприниматели проводят проверки подразделений ОАО «РЖД» в установленном ОАО «РЖД» порядке в соответствии с условиями договора и технического задания к нему, либо привлекаются к работе комиссии в качестве экспертов.

22. Проверки подразделяются на плановые, внеплановые и контрольные. Длительность проверки не может превышать 20 календарных дней. При необходимости срок проверки может быть продлен ответственным за организацию обработки персональных данных в ОАО «РЖД» или руководителем подразделения ОАО «РЖД», подписавшим предписание о проведении проверки, на срок не более 20 дней.

23. Допускается проведение проверки одновременно в нескольких подразделениях ОАО «РЖД».

24. Планы проверок подразделений ОАО «РЖД» формируются ответственными за организацию обработки персональных данных по форме согласно приложению № 1 и утверждаются руководителями этих подразделений.

Региональные (структурные) подразделения филиалов и структурных подразделений ОАО «РЖД», расположенные в границах железных дорог, копии утвержденных планов проверок направляют в соответствующие филиалы и структурные подразделения ОАО «РЖД».

Филиалы и структурные подразделения ОАО «РЖД», имеющие в своем составе (ведении) региональные (структурные) подразделения, в планы проверок включают проверки, планируемые данными подразделениями.

В случае планирования филиалами и структурными подразделениями ОАО «РЖД» проведения проверок в региональных (структурных) подразделениях, входящих в их состав (находящихся в ведении), выписки из планов проверок направляются руководителям соответствующих подразделений.

25. В срок до 1 декабря текущего года подразделения аппарата управления, филиалы и структурные подразделения ОАО «РЖД» направляют копии планов проверок в Управление.

26. План проверок соблюдения режима защиты персональных данных подразделений ОАО «РЖД», проводимых Управлением, утверждается ответственным за организацию обработки персональных данных в ОАО «РЖД» ежегодно, не позднее 15 января текущего года, по форме согласно приложению № 2. Выписка из плана проверок направляется руководителям подразделений ОАО «РЖД», в которых запланировано проведение проверок.

27. Для проведения проверки издается приказ по форме согласно приложению № 3, в соответствии с которым образуется комиссия по проведению проверки соблюдения режима защиты персональных данных (далее также – комиссия) численностью не менее 3 человек.

Комиссия готовит перечень вопросов, рассматриваемых в ходе проверки.

28. Для проведения проверки соблюдения режима защиты персональных данных на железных дорогах образуются комиссии, в состав которых могут быть включены работники подразделений органов управления (служб управления персоналом, корпоративной информатизации, юридической службы и др.), структурных подразделений железной дороги, представители региональных (структурных) подразделений.

29. Не допускается включение в состав комиссии работников, не уполномоченных на обработку персональных данных.

30. Основанием для проведения проверки соблюдения режима защиты персональных данных является составленное в 2 экземплярах предписание о проведении проверки.

Для проверок, проводимых Управлением, составляется предписание по форме согласно приложению № 4, которое подписывается ответственным за организацию обработки персональных данных в ОАО «РЖД».

Для проверок, проводимых филиалами или структурными подразделениями ОАО «РЖД», составляется предписание на бланке подразделения по форме согласно приложению № 5, которое подписывается руководителем филиала или структурного подразделения ОАО «РЖД».

31. Руководитель подразделения ОАО «РЖД», в котором запланировано проведение проверки, письменно уведомляется Управлением, филиалом

или структурным подразделением ОАО «РЖД» о проверке не менее, чем за 10 рабочих дней до ее начала.

В уведомлении, составленном по форме согласно приложению № 6, указываются сроки проведения проверки, требования к организации ее проведения, а также перечень вопросов, рассматриваемых в ходе проверки.

32. Проверки в подразделениях аппарата управления ОАО «РЖД», органах управления филиалов и структурных подразделений ОАО «РЖД», региональных (структурных) подразделениях филиалов и структурных подразделений ОАО «РЖД», расположенных в границах железных дорог, проводятся на основании приказа об образовании комиссии по проведению проверки режима защиты персональных данных, подготовленному в соответствии с пунктом 27, без оформления предписания и уведомления о проверке.

33. Внеплановая проверка в подразделениях ОАО «РЖД» проводится по указанию генерального директора – председателя правления ОАО «РЖД» либо ответственного за обработку персональных данных в ОАО «РЖД», а также руководителя подразделения ОАО «РЖД» в случае наличия инцидента, связанного с нарушениями режима защиты персональных данных.

34. Контрольная проверка в подразделениях ОАО «РЖД» проводится для оценки полноты устранения нарушений, выявленных в ходе плановой или внеплановой проверки, после завершения мероприятий, по устранению выявленных нарушений, но не позднее одного года с даты завершения проверки.

35. В случае выявления в ходе проверки фактов утраты материальных носителей персональных данных, распространения либо неправомерной обработки персональных данных субъектов персональных данных проводится служебное расследование в установленном ОАО «РЖД» порядке.

IV. Права, обязанности и ответственность комиссии по проведению проверки соблюдения режима защиты персональных данных

36. Члены комиссии руководствуются при проведении проверки настоящим Положением и другими нормативными и методическими документами ОАО «РЖД».

37. Председатель комиссии:

1) в день начала проверки представляет руководителю подразделения ОАО «РЖД», в котором будет проведена проверка, членов комиссии, доводит информацию о порядке проведения проверки и передает для ознакомления и подписания предписание о проведении проверки в двух экземплярах. Второй экземпляр предписания с подписью руководителя проверяемого подразделения

остается у председателя комиссии для дальнейшего приобщения к материалам проверки;

2) организует взаимодействие с руководителем проверяемого подразделения и ответственным за организацию обработки персональных данных в этом подразделении по вопросам, рассматриваемым в ходе проверки;

3) устанавливает по согласованию с руководителем проверяемого подразделения время ежедневного пребывания членов комиссии в служебных помещениях в течение срока проверки с учетом режима работы этого подразделения;

4) по согласованию с начальником Управления (руководителем подразделения ОАО «РЖД», подписавшим предписание о проведении проверки) может ознакомить руководителя проверяемого подразделения с проектом акта проверки и иными материалами проверки до ее завершения.

38. Члены комиссии имеют право:

1) входить в служебные помещения проверяемого подразделения в сопровождении работников этого подразделения;

2) пользоваться необходимыми для проведения проверки техническими средствами;

3) запрашивать в проверяемом подразделении необходимые для проведения проверки документы (сведения);

4) проводить беседы и консультации с работниками проверяемого подразделения, требовать предоставления письменных справок, отчетов по вопросам, рассматриваемым в ходе проверки;

5) снимать копии с документов проверяемого подразделения для приобщения к материалам проверки;

6) знакомиться с документацией на автоматизированные рабочие места и информационные системы, используемые при обработке персональных данных, проверяемым подразделением;

7) запрашивать от работников проверяемого подразделения информацию о функционировании автоматизированных рабочих мест и информационных систем, используемых при обработке персональных данных;

8) требовать от работников проверяемого подразделения демонстрации своей работы на автоматизированных рабочих местах с информационными системами при обработке персональных данных и производить выборку необходимой информации;

9) направлять запросы в другие подразделения ОАО «РЖД» с целью получения дополнительной информации по вопросам, рассматриваемым в ходе проверки.

39. Члены комиссии несут ответственность в соответствии с законодательством Российской Федерации за разглашение полученных в ходе

проверки сведений, содержащих персональные данные, и иной информации ограниченного доступа.

40. При привлечении Управлением для проведения проверок третьих лиц, в соответствии с пунктом 20 настоящего Положения, в том числе в составе комиссии, на них распространяются права, и они несут ответственность, предусмотренные пунктами 38 и 39 настоящего Положения соответственно.

V. Обязанности руководителя и работников подразделений ОАО «РЖД», в которых проводится проверка

41. Руководитель подразделения ОАО «РЖД», в котором проводится проверка:

1) информирует работников подразделения о цели и характере проверки;

2) определяет работников подразделения для работы с членами комиссии;

3) обеспечивает доступ к документам (сведениям) в ходе проведения проверки, а также иные условия для проведения проверки.

42. Руководитель и работники проверяемого подразделения в период проверки обязаны:

1) содействовать комиссии в проведении проверки;

2) обеспечивать беспрепятственный доступ членов комиссии в служебные помещения проверяемого подразделения;

3) предоставлять при необходимости членам комиссии рабочие места в служебном помещении проверяемого подразделения;

4) демонстрировать членам комиссии свою работу на автоматизированных рабочих местах с информационными системами, содержащими персональные данные, включая выборку необходимой информации;

5) предоставлять документы (сведения), необходимые для проведения проверки, в сроки, установленные председателем комиссии.

43. В случае отсутствия документов (сведений), необходимых для проведения проверки, и (или) возникновения обстоятельств, препятствующих их предоставлению, руководитель подразделения ОАО «РЖД», в котором проводится проверка, представляет председателю комиссии письменное объяснение с указанием причин.

VI. Оформление результатов проверки соблюдения режима защиты персональных данных, порядок разработки, утверждения и исполнения плана устранения нарушений

44. По результатам проведения проверки составляется в двух экземплярах акт на бланке подразделения ОАО «РЖД», проводившего проверку, по форме согласно приложению № 7.

Сведения о проверке отражаются в журнале учета проверок соблюдения режима защиты персональных данных подразделения ОАО «РЖД» по форме согласно приложению № 8, как в проверяемом, так и в проверяющем подразделении.

45. Основная часть акта проверки содержит информацию о рассмотренных в ходе проверки вопросах с обязательным отражением по каждому из них следующих сведений:

1) о выполнении в проверяемом подразделении ОАО «РЖД» требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области обработки и обеспечении безопасности персональных данных, принятых мерах по обеспечению безопасности персональных данных;

2) о выявленных нарушениях режима защиты персональных данных;

3) об устраненных на дату завершения проверки нарушениях.

46. Заключительная часть акта проверки содержит выводы комиссии по результатам проведения проверки.

Документы, подтверждающие выявленные в ходе проверки нарушения, при необходимости приобщаются к акту.

47. Акт проверки составляется не позднее 10 рабочих дней с даты окончания проверки и подписывается председателем и членами комиссии.

В случае невозможности подписания акта проверки каким-либо членом комиссии (болезнь, отпуск, служебная командировка, иные объективные причины) председатель комиссии делает в акте соответствующую отметку.

Акт проверки подлежит регистрации в системе ЕАСД. В карточке документа проставляется отметка «Ограниченный доступ».

Акт проверки направляется в подразделение ОАО «РЖД», в котором проводилась проверка, по ЕАСД с сопроводительным письмом. При этом к карточке письма прикрепляется файл сканированного акта проверки, подписанный членами комиссии. В карточке документа проставляется отметка «Ограниченный доступ».

В случае отсутствия в подразделении, в котором проводилась проверка, системы ЕАСД, в карточке письма в ЕАСД указывается, что документ направляется в бумажном виде, при этом файл сканированного акта проверки к карточке не прикрепляется.

Оба экземпляра акта проверки не позднее 2 рабочих дней с даты подписания направляются с сопроводительным письмом в запечатанном конверте руководителю подразделения, в котором проводилась проверка. Один экземпляр акта с отметкой об ознакомлении подлежит возврату отправителю.

48. Руководитель или ответственный за организацию обработки персональных данных подразделения ОАО «РЖД», в котором проводилась проверка, не позднее 10 рабочих дней с даты получения акта проверки, рассматривает его и утверждает план устранения выявленных нарушений по форме согласно приложению № 9. План направляется в Управление или руководителю подразделения ОАО «РЖД», подписавшему предписание о проведении проверки.

Датой получения акта проверки считается дата поступления его по ЕАСД, а в случае отсутствия ЕАСД - дата регистрации входящего документа.

49. По результатам проверки председатель комиссии представляет начальнику Управления (руководителю подразделения ОАО «РЖД», подписавшему предписание (приказ) о проведении проверки) докладную записку с приложением акта проверки.

50. Мероприятия, предусмотренные планом по устранению нарушений, не влекущие за собой дополнительного финансирования и не требующие согласования с соответствующими подразделениями ОАО «РЖД», должны быть исполнены подразделением ОАО «РЖД», в котором проводилась проверка, в течение одного месяца с даты ознакомления с актом проверки руководителя или ответственного за организацию обработки персональных данных в этом подразделении.

51. Отчет подразделения, в котором проводилась проверка, об исполнении плана устранения нарушений направляется в Управление (руководителю подразделения ОАО «РЖД», подписавшему предписание (приказ) о проведении проверки) не позднее 5 рабочих дней со дня истечения срока, предусмотренного указанным планом.

VII. Формирование отчетности о контроле за соблюдением режима защиты персональных данных

52. Ответственные за организацию обработки персональных данных в подразделениях аппарата управления, филиалах и структурных подразделениях ОАО «РЖД» формируют и представляют в Управление отчетные документы в виде статистического отчета о контроле за соблюдением режима защиты персональных данных, пояснительной записки к нему по форме согласно приложению № 10 и аналитической справки, содержащей:

результаты мониторинга и проверок;

информацию о характере выявленных нарушений требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области персональных данных;

информацию о проверках контрольно-надзорных органов и составленных ими административных протоколах;

сведения о мерах, принятых для устранения выявленных нарушений;

выводы о состоянии защищенности персональных данных;

предложения по совершенствованию режима защиты персональных данных и повышению уровня их защищенности;

Указанные документы по итогам первого полугодия направляются в Управление до 15 июля текущего года, по итогам года – до 15 января следующего года.

53. Региональные (структурные) подразделения филиалов и структурных подразделений ОАО «РЖД», расположенные в границах железных дорог, направляют в адрес подразделений ОАО «РЖД», в состав которых они входят или в ведении которых они находятся, сведения о результатах мониторинга и проверок.

Ответственные за организацию обработки персональных данных в филиалах и структурных подразделениях ОАО «РЖД» включают полученные сведения в состав аналитических справок и статистических отчетов о результатах контроля.

54. По итогам обобщения отчетных документов Управление информирует ответственного за организацию обработки персональных данных в ОАО «РЖД» о состоянии режима защиты персональных данных в ОАО «РЖД» и о предложениях по проведению мероприятий по воздействию на выявленные риски для их минимизации (устранения), а также предотвращения их повторного возникновения и реализации.

Приложение № 1
к Положению о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД»

УТВЕРЖДАЮ

_____
Руководитель подразделения ОАО «РЖД»
(подпись) И.О.Фамилия
(дата)

ПЛАН
проведения проверок соблюдения режима защиты персональных данных

в _____ в 20__ году
(наименование подразделения ОАО «РЖД»)

№ п/п	Наименование подразделения аппарата управления, филиала, структурного подразделения ОАО «РЖД»	Адрес объекта проверки	Основание проверки	Период проведения проверки		Принимающие участие в проведении проверки подразделения ОАО «РЖД», ДЗО, юридические лица, индивидуальные предприниматели	Форма проведения проверки (документарная, выездная, документарная и выездная)
				Дата начала проверки	Срок проведения проверки		
1							

Должность –
ответственный за организацию обработки персональных данных (подпись) И.О.Фамилия

Приложение № 2
к Положению о контроле за соблюдением
режима защиты персональных данных
в ОАО «РЖД»

УТВЕРЖДАЮ
Заместитель генерального директора ОАО
«РЖД» - ответственный за организацию
обработки персональных данных в ОАО «РЖД»
_____ И.О.Фамилия
« ___ » _____ 20__ г.

ПЛАН
проведения проверок соблюдения режима защиты персональных данных в подразделениях ОАО «РЖД» на 20__ год

№ п/п	Наименование подразделения аппарата управления, филиала, структурного подразделения ОАО «РЖД»	Адрес объекта проверки	Основание для проведения проверки	Период проведения проверки		Принимающие участие в проведении проверки подразделения ОАО «РЖД», ДЗО, юридические лица, индивидуальные предприниматели	Форма проведения проверки (документарная, выездная, документарная и выездная)
				Дата начала проверки	Срок проведения проверки		
1							

Начальник Управления
по защите персональных данных И.О.Фамилия

Приложение № 3
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

ОАО «РЖД»
ДЕПАРТАМЕНТ СОЦИАЛЬНОГО РАЗВИТИЯ

ПРИКАЗ

_____г. № _____

**Об образовании комиссии
по проведению проверки соблюдения режима защиты персональных данных в _____**
(наименование подразделения ОАО «РЖД»)

В соответствии с Положением о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от __ _____ 20__ г. № _____ (далее – Положение), и планом проверок на 20__ год от ___ _____ 20__ г. № __ п р и к а з ы в а ю:

1. Образовать комиссию по проведению проверки соблюдения режима защиты персональных данных в Департаменте социального развития в составе:

Фамилия И.О. – _____ (председатель комиссии)
(должность, Ф.И.О.)

Фамилия И.О. – _____
(должность, Ф.И.О.)

Фамилия И.О. – _____
(должность, Ф.И.О.)

2. Членам комиссии руководствоваться при проведении проверки Положением и другими нормативными документами ОАО «РЖД».

Руководитель_____ И.О.Фамилия
(подразделения ОАО «РЖД»)

Приложение № 4
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

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

_____г. №_____

ПРЕДПИСАНИЕ
о проведении проверки

В соответствии с Положением о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от _____ 20__ г. №____р и планом проведения проверок в подразделениях аппарата управления, филиалах и структурных подразделениях ОАО «РЖД» на ____ год от _____ № ___, комиссии в составе:

Фамилия И.О. – _____ (председатель комиссии)
(должность)

Фамилия И.О. – _____
(должность)

Фамилия И.О. – _____
(должность)

Фамилия И.О. – _____
(должность)

поручается провести в период с ___ по ___ проверку соблюдения режима защиты персональных данных в _____.
(наименование подразделения ОАО «РЖД»)

Вопросы, рассматриваемые в ходе проверки

_____

Предписание действительно с _____ до _____ 20 ___ г.

Заместитель генерального директора
ОАО «РЖД» _____ И.О.Фамилия
(подпись)

«___» _____ 20__ г.

Печать

Предписание получено «_____» _____ 20___ г.

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

Приложение № 5
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

ОАО «РЖД»
ДЕПАРТАМЕНТ ТЕХНИЧЕСКОЙ ПОЛИТИКИ

ПРЕДПИСАНИЕ

_____г. № _____

В соответствии с Положением о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от _____ 20__ г. № _____р и _____
(основание для проведения проверки)
комиссии в составе:

Фамилия И.О. – _____ (председатель комиссии)
(должность)

Фамилия И.О. – _____
(должность)

Фамилия И.О. – _____
(должность)

поручается провести в период с ___ по ___ проверку соблюдения режима защиты персональных данных в _____.
(наименование подразделения ОАО «РЖД»)

Вопросы, рассматриваемые в ходе проверки

_____.

Предписание действительно с _____ до _____ 20___ г.

Руководитель_____ И.О.Фамилия
(подразделения ОАО «РЖД»)

«___» _____ 20___ г.

Печать

Предписание получено «_____» _____ 20___ г.

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

Приложение № 6
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

ОАО «РЖД»
ЦЕНТРАЛЬНАЯ ДИРЕКЦИЯ ЗДРАВООХРАНЕНИЯ

Начальнику_____
(наименование подразделения)

УВЕДОМЛЕНИЕ

_____г. № _____

О проведении проверки

Уважаемый _____!

Сообщаем, что в соответствии с планом проверок на 20__ год от ___ _____ 20__ г. № __ в период с __ по __ _____ 20__ Центральной дирекцией здравоохранения будет проводиться проверка соблюдения режима защиты персональных данных в _____.
(наименование подразделения)

В соответствии с разделом V Положения о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД», утвержденного распоряжением ОАО «РЖД» от _____ № _____, просим обеспечить условия для проведения проверки, оперативное представление необходимых сведений и документов, организовать доступ к оборудованию, используемому для обработки персональных данных, и в соответствующие помещения.

Приложение: Перечень вопросов, подлежащих проверке, на __ л.

Руководитель_____ И.О.Фамилия
(подразделения ОАО «РЖД»)

Приложение № 7
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

Экз.

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

АКТ ПРОВЕРКИ

Дата начала проверки «___»_____ 20___ г.
Дата окончания проверки «___»_____ 20___ г.

Место проведения проверки _____.
(адрес проверяемого подразделения ОАО «РЖД»)

Настоящий акт составлен по результатам проверки соблюдения режима защиты персональных данных в _____,
(наименование подразделения ОАО «РЖД»)
проведенной комиссией в составе:

Фамилия И.О. – _____ (председатель комиссии)
(должность)
Фамилия И.О. – _____
(должность)
Фамилия И.О. – _____
(должность)
на основании _____.

В ходе проверки рассмотрены следующие вопросы:

_____
(основная часть согласно п. п.26,44 Положения)

Выводы по результатам проверки

_____.

Приложение:_____ на _____ л.
(с указанием прилагаемых документов и их копий)
Настоящий акт составлен в двух экземплярах.

Председатель комиссии _____ _____
(подпись) (расшифровка подписи)
Члены комиссии: _____ _____
(подпись) (расшифровка подписи)

(подпись)	(расшифровка подписи)
(подпись)	(расшифровка подписи)

«___»_____ 20___ г.

С актом проверки ознакомлен:

(должность)	(подпись)	(расшифровка подписи)

«___»_____ 20___ г.

Приложение № 8
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

ЖУРНАЛ
учета проверок соблюдения режима защиты персональных данных

_____
(наименование подразделения ОАО «РЖД»)

п/п	Наименование проверяемого подразделения	Адрес места нахождения объекта проверки	№ и дата предписания о проведении проверки	Подразделение (контрольно-надзорный орган) проводившее проверку	№ и дата составления акта проверки	№ и дата Плана устранения нарушений	№ дела, где хранятся материалы проверки
1	2	3	4	5	6	7	8

Приложение № 9
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

УТВЕРЖДАЮ

_____
Руководитель подразделения ОАО «РЖД»

(подпись) И.О.Фамилия
(дата)

ПЛАН

устранения нарушений, выявленных в ходе проверки соблюдения режима защиты персональных данных

В _____
(наименование подразделения ОАО «РЖД»)

№ п/п	Нарушение	Мероприятия по устранению нарушений	Ответственный	Срок исполнения	Примечание

Должность –
ответственный за организацию обработки персональных данных (подпись) И.О.Фамилия

Приложение № 10
к Положению о контроле
за соблюдением режима
защиты персональных
данных в ОАО «РЖД»

СТАТИСТИЧЕСКИЙ ОТЧЕТ
о контроле за соблюдением режима защиты персональных данных

в _____
(наименование подразделения ОАО «РЖД»)

за _____
(период)

№ п/п	Сведения	Количество
1.	Проверки, проведенные контролирующими и надзирающими органами	
1.1.	Роскомнадзор	
1.2.	ФСБ России	
1.3.	ФСТЭК России	
1.4.	Прокуратура	
2.	Получено предписаний об устранении нарушений, выявленных контролирующими и надзирающими органами	
2.1.	Роскомнадзор	
2.2.	ФСБ России	
2.3.	ФСТЭК России	
2.4.	Прокуратура	
3.	Получено протоколов об административных правонарушениях от контролирующих и надзирающих органов	
3.1.	Роскомнадзор	
3.2.	ФСБ России	
3.3.	ФСТЭК России	
3.4.	Прокуратура	
4.	Проведено внутренних проверок	
5.	Рассмотрено обращений (запросов) субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных о нарушениях обработки персональных данных	
6.	Выявлено нарушений режима защиты персональных данных	
7.	Проведено служебных расследований	
7.1.	По фактам утраты материальных носителей персональных данных	

№ п/п	Сведения	Количество
7.2.	По фактам распространения персональных данных	
7.3.	По фактам неправомерной обработки персональных данных	
8.	Привлечено к дисциплинарной и (или) материальной ответственности	
9.	Направлено обращений в правоохранительные органы в отношении лиц, допустивших утрату материальных носителей персональных данных, разглашение либо неправомерную обработку персональных данных субъектов персональных данных	
10.	Заключено договоров с третьими лицами на обработку персональных данных	
11.	Количество фактов трансграничной передачи[1] персональных данных	

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА[2]

к статистическому отчету о контроле за соблюдением режима защиты персональных данных

К статистическому отчету прилагается пояснительная записка, содержащая следующую информацию:

по подпунктам 1.1–1.4 – указываются вид проверок, их сроки, мероприятия по контролю, проведенные в ходе проверок, сведения об отсутствии или наличии нарушений с наименованием вида нарушения и нарушенных нормативно-правовых актов;

по подпунктам 2.1–24 – перечисляются полученные предписания об устранении выявленных нарушений, включая сведения о нарушениях и сроках их устранения;

по подпунктам 3.1–3.4 – перечисляются полученные протоколы об административных правонарушениях с указанием следующих сведений: кем, в отношении кого составлен протокол, событие административного правонарушения со ссылкой на нарушенные нормы законодательства, результаты рассмотрения дела;

по пункту 4 – перечисляются проведенные проверки с указанием их вида, сроков и результатов;

---

[1] Трансграничная передача – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или юридическому лицу.

[2] К позициям статистического отчета, информация по которым отсутствует, пояснений не требуются. В случае, если по всем пунктам статистического отчета сведения о контроле за соблюдением режима защиты персональных данных отсутствуют, пояснительная записка не составляется.

по пункту 5 – излагается суть и результаты рассмотренных обращений (запросов) субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных о нарушениях обработки персональных данных;

по пункту 6 – дается краткое описание выявленных в ходе мониторинга и проверок нарушений режима защиты персональных данных как при автоматизированной, так и неавтоматизированной обработке персональных данных, со ссылкой на нарушенные нормы законодательства и нормативные документы ОАО «РЖД» в области обработки и защиты персональных данных;

по подпунктам 7.1–7.3 – указываются сведения, содержащиеся в заключении о результатах проведенных служебных расследований по фактам утраты материальных носителей, распространения либо неправомерной обработки персональных данных;

по пункту 8 – указываются сведения о привлечении виновных работников ОАО «РЖД» к дисциплинарной и (или) материальной ответственности по результатам служебных расследований;

по пункту 9 – дается краткое описание материалов, требующих уголовно-правового, административного или иного преследования уполномоченными органами государства и направленных по инициативе руководителя подразделения ОАО «РЖД» в правоохранительные и контролирующие органы, в отношении лиц, допустивших утрату материальных носителей персональных данных, распространение либо неправомерную обработку персональных данных, с указанием принятых по ним решений;

по пункту 10 – указываются реквизиты договоров, заключенных с третьими лицами, на обработку персональных данных;

по пункту 11 – указываются названия иностранных государств, на территорию которых осуществлялась трансграничная передача, состав персональных данных и цели трансграничной передачи.

Дополнительно при трансграничной передаче персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, указываются случаи осуществления трансграничной передачи в соответствии с пунктом 70 Порядка обработки и обеспечения режима защиты персональных данных работников ОАО «РЖД», утвержденного приказом ОАО «РЖД» от 20 июля 2016 г. № 60.

Ответственный за организацию
обработки персональных данных

_____ _____ И.О.Фамилия

(наименование подразделения ОАО «РЖД») (подпись)

«___»_____ 20___ г.