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

РАСПОРЯЖЕНИЕ

7 марта 2024 г. Москва № 615/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 корпоративного управления Евсегнеевой В.А. и заместителю начальника Центра по корпоративному управлению пригородным комплексом Заглядовой Т.И. довести Положение до сведения руководителей хозяйственных обществ с участием ОАО «РЖД» по перечню согласно приложению № 1 и руководителей пригородных пассажирских компаний – хозяйственных обществ с участием ОАО «РЖД» по перечню согласно приложению № 2 для использования в своей деятельности и при разработке или актуализации соответствующих внутренних документов, а также доведения до сведения собственных подконтрольных обществ.

4. Признать утратившими силу:

распоряжение ОАО «РЖД» от 2 декабря 2019 г. № 2719/р «Об утверждении Положения о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД»;

распоряжение ОАО «РЖД» от 21 июля 2020 г. № 1553/р «О внесении изменений в Положение о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД».

5. 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. Маханьков И.Е., ЦИБ
(499) 262-50-83

УТВЕРЖДЕНО
распоряжением ОАО «РЖД»
от «7» марта 2024 г. № 615/р

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

I. Общие положения

1. Настоящее Положение, разработанное в соответствии с законодательством 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» (далее – подразделения ОАО «РЖД»), а также в региональных (структурных) подразделениях филиалов и структурных подразделений ОАО «РЖД», расположенных в границах железных дорог (далее – региональные подразделения).

2. В настоящем Положении используются следующие понятия:

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

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

компьютерный инцидент – факт нарушения и (или) прекращения функционирования информационного ресурса, сети связи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе информации, в том числе произошедший в результате компьютерной атаки;

контроль за соблюдением режима защиты персональных данных – совокупность действий по мониторингу и проверке соблюдения режима защиты персональных данных;

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;

обеспечение безопасности персональных данных – деятельность, 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;

проверка соблюдения режима защиты персональных данных – комплекс мероприятий, направленных на выявление нарушений режима защиты персональных данных либо установление отсутствия таких нарушений в подразделениях ОАО «РЖД» (региональных подразделениях);

риск, связанный с нарушением режима защиты персональных данных, – потенциальная опасность нанесения ОАО «РЖД» ущерба 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 является оценка в рамках рискориентированного подхода соответствия обработки и обеспечения безопасности персональных данных требованиям законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области персональных данных.

4. Задачи контроля за соблюдением режима защиты персональных данных:

1) анализ выполнения требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области 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 осуществляют Департамент управления информационной безопасностью (далее – Департамент), ответственные за организацию обработки персональных данных в подразделениях ОАО «РЖД» и региональных подразделениях, а также ответственные за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД» путем проведения мониторинга и проверок соблюдения режима защиты персональных данных.

6. Ответственные за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД» организуют контроль за соблюдением Требований к защите персональных данных при их

обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, не реже 1 раза в 3 года как самостоятельно, так и с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7. Департамент осуществляет координацию деятельности:

ответственных за организацию обработки персональных данных в подразделениях ОАО «РЖД»;

ответственных за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД»;

комитетов по организации обработки и обеспечению безопасности персональных данных региональных оперативных комиссий по координации взаимодействия железных дорог с региональными подразделениями функциональных филиалов, структурными подразделениями, учреждениями ОАО «РЖД», а также хозяйственными обществами с участием ОАО «РЖД» (далее – комитеты РОК).

8. Ответственные за организацию обработки персональных данных в филиалах и структурных подразделениях ОАО «РЖД» и комитеты РОК осуществляют координацию деятельности ответственных за организацию обработки персональных данных в региональных подразделениях.

9. При проведении проверок соблюдения законодательства Российской Федерации в области персональных данных контрольными (надзорными) органами государственной власти (Минцифры России, Роскомнадзор, ФСТЭК России, ФСБ России, органы прокуратуры Российской Федерации) руководителям подразделений ОАО «РЖД» и региональных подразделений 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 от контрольного (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 Департамент 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 письменно уведомляет Департамент о фактах привлечения ОАО «РЖД» или его должностных лиц к административной или уголовной ответственности за нарушение требований законодательства Российской Федерации в области персональных данных.

II. Мониторинг соблюдения режима защиты персональных данных

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

13. Департамент во взаимодействии с ответственными за обеспечение безопасности персональных данных в информационных системах ОАО «РЖД» в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, осуществляет мониторинг:

своевременности установления уровня защищенности персональных данных при их обработке в информационной системе ОАО «РЖД»;

проведения оценки эффективности реализованных в информационной системе ОАО «РЖД» мер по обеспечению безопасности обрабатываемых в ней персональных данных.

14. Департамент вправе осуществлять мониторинг без взаимодействия с подразделениями ОАО «РЖД».

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

1) соблюдения порядка организации допуска к персональным данным;

2) соблюдения требований конфиденциальности и обеспечения безопасности при обработке персональных данных;

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

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

5) включения в должностные инструкции работников, уполномоченных на обработку персональных данных, соответствующих обязанностей;

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

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

8) наличия согласий субъектов персональных данных на их обработку (передачу);

9) актуальности перечней помещений, в которых обрабатываются персональные данные (хранятся материальные носители персональных данных);

10) учета машинных носителей персональных данных;

11) актуальности сведений, содержащихся в Паспорте оператора персональных данных подразделения ОАО «РЖД»;

12) организации работы с обращениями (запросами) субъектов персональных данных, юридических лиц и контрольных (надзорных) органов по вопросам обработки персональных данных.

Результаты мониторинга оформляются аналитической справкой, подготовленной в соответствии с пунктом 56 настоящего Положения.

16. Ответственный за организацию обработки персональных данных в подразделении ОАО «РЖД» (региональном подразделении) незамедлительно информирует руководителя соответствующего подразделения и Департамент об обнаружении факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей за собой нарушение прав субъектов персональных данных, либо о поступлении такой информации от Роскомнадзора, иного органа власти или заинтересованного лица.

17. Ответственный за обеспечение безопасности персональных данных в информационной системе ОАО «РЖД» незамедлительно информирует руководителя соответствующего подразделения (функционального заказчика), Департамент и Центр компетенций по информационной безопасности

о компьютерных инцидентах, повлекших за собой неправомерную передачу (предоставление, распространение, доступ) персональных данных.

18. 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.

19. По факту выявленных в процессе мониторинга рисков, связанных с нарушениями режима защиты персональных данных, руководством подразделения, проводившего мониторинг, принимаются меры по их минимизации (устранению).

III. Организация и проведение проверок соблюдения режима защиты персональных данных

20. Проверки соблюдения режима защиты персональных данных организуют Департамент, ответственные за организацию обработки персональных данных в подразделениях ОАО «РЖД» (региональных подразделениях), а также комитеты РОК.

21. Для проведения проверок, 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 установленном порядке могут привлекаться работники подразделений ОАО «РЖД», хозяйственных обществ с участием ОАО «РЖД» с учетом специфики их деятельности, а также на договорной основе юридические лица и индивидуальные предприниматели.

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

23. Проверки подразделяются на плановые, внеплановые и контрольные.

Длительность проверки не может превышать 20 календарных дней.

Руководитель подразделения ОАО «РЖД» (регионального подразделения), подписавший предписание о проведении проверки, может изменить срок проведения проверки, в том числе продлить ее, по представлению председателя комиссии по проведению проверки соблюдения режима защиты

персональных данных на срок не более 20 календарных дней с внесением изменений в предписание о проведении проверки. При необходимости срок проверки может быть продлен в установленном порядке ответственным за организацию обработки персональных данных в ОАО «РЖД» или руководителем подразделения ОАО «РЖД» (регионального подразделения), подписавшим предписание о проведении проверки, на срок не более 20 календарных дней.

24. Планы проведения проверок подразделений ОАО «РЖД» и региональных подразделений (далее – планы проверок) формируются ответственными за организацию обработки персональных данных в подразделениях ОАО «РЖД» и региональных подразделениях по форме согласно приложению № 1 и утверждаются руководителями этих подразделений.

Региональные подразделения направляют копии утвержденных планов проверок, в том числе имеющихся в их составе структурных подразделений, в соответствующие филиалы и структурные подразделения ОАО «РЖД», которые включают их в свой план проверок.

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

По указанию председателя комитета РОК формируется план проверок в региональных подразделениях по форме, указанной в приложении № 1 к настоящему Положению, который утверждается ответственным за организацию обработки персональных данных на железной дороге. Выписки из плана проверок направляются руководителям соответствующих подразделений.

25. Периодичность проведения проверок определяется исходя из анализа контрольной деятельности за текущий год (результатов мониторинга процессов обработки и обеспечения безопасности персональных данных, проверок, характера и систематичности выявляемых нарушений).

В случае невыявления в ходе проведения внутреннего контроля за соблюдением режима защиты персональных данных нарушений, которые могут привести к распространению либо неправомерной обработке персональных данных, утрате их материальных носителей, допускается проведение проверки 1 раз в 3 года.

26. Подразделения ОАО «РЖД» и комитеты РОК в срок до 1 декабря текущего года направляют в Департамент копии планов проверок на следующий год.

27. План проверок подразделений ОАО «РЖД», проводимых Департаментом, разрабатывается при необходимости на основании результатов мониторинга по форме согласно приложению № 2 и утверждается ответственным за организацию обработки персональных данных в ОАО «РЖД». Выписки из плана проверок направляются руководителям подразделений ОАО «РЖД», в которых запланировано проведение проверок.

28. Для проведения проверки образуется комиссия по проведению проверки соблюдения режима защиты персональных данных (далее – комиссия) численностью не менее 3 человек путем издания приказа по форме согласно приложению № 3.

Комиссия может быть образована на неопределенный срок либо на определенный период (на период проведения проверки).

Комиссия готовит перечень вопросов, рассматриваемых в ходе проверки.

29. Для проведения проверок в региональных подразделениях согласно плану проверок комитета РОК приказом, подготовленным в соответствии с пунктом 28 настоящего Положения, образуется комиссия, в состав которой могут быть включены работники подразделений органов управления (службы управления персоналом, корпоративной информатизации, юридической службы и др.), структурных подразделений железной дороги, работники региональных центров безопасности и других региональных подразделений.

30. Запрещается включение в состав комиссии работников, не уполномоченных на обработку персональных данных.

31. Основанием для проведения проверки является составленное в 2 экземплярах предписание о проведении проверки.

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

Для проверок, проводимых подразделениями ОАО «РЖД» в подчиненных им региональных подразделениях, оформляется предписание на бланке подразделения ОАО «РЖД» по форме согласно приложению № 5, которое подписывается руководителем подразделения ОАО «РЖД».

Для проверок, проводимых региональными подразделениями в подчиненных им структурных подразделениях, оформляется предписание на бланке регионального подразделения по форме, указанной в приложении № 5 к настоящему Положению, которое подписывается руководителем регионального подразделения.

Для проверок, проводимых согласно планам комитетов РОК, оформляется предписание по форме, указанной в приложении № 5 к настоящему Положению, которое подписывается председателем комитета РОК.

32. Руководитель подразделения ОАО «РЖД» (регионального подразделения), в котором запланировано проведение проверки, письменно уведомляется о проверке не менее чем за 10 рабочих дней до ее начала тем подразделением, которое будет проводить проверку.

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.

33. Для подразделений ОАО «РЖД», не имеющих в своем составе (ведении) региональных подразделений, оформление предписания о проведении проверки и уведомления о проведении проверки не требуется.

34. 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» (регионального подразделения).

35. Контрольная проверка в подразделениях ОАО «РЖД» (региональных подразделениях) проводится (при необходимости) 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.

36. В случае выявления в ходе проверки фактов утраты материальных носителей персональных данных, распространения либо неправомерной обработки персональных данных, а также предпосылок к ним в установленном порядке проводится служебное расследование.

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

37. При проведении проверки члены комиссии руководствуются настоящим Положением и другими нормативными и методическими документами ОАО «РЖД».

38. Председатель комиссии:

в день начала проверки представляет руководителю подразделения, в котором будет проведена проверка (далее – проверяемое подразделение), членов комиссии, доводит до его сведения информацию о порядке проведения проверки и передает (при наличии) 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;

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

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;

по согласованию с руководителем, подписавшим предписание о проведении проверки, либо директором ОАО «РЖД» – начальником Департамента управления информационной безопасностью (в случае проведения проверки Департаментом) может ознакомить руководителя проверяемого подразделения с проектом акта проверки и иными материалами проверки до ее завершения.

39. Члены комиссии имеют право:

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

пользоваться необходимыми для проведения проверки техническими средствами;

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

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

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

знакомиться с документацией на автоматизированные рабочие места и информационные системы, используемые при обработке персональных данных в проверяемом подразделении;

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

требовать от работников проверяемого подразделения демонстрации своей работы на автоматизированных рабочих местах в информационных системах, используемых при обработке персональных данных, и осуществлять выборку необходимой информации;

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

40. 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.

41. При привлечении к проведению проверок третьих лиц в соответствии с пунктом 21 настоящего Положения, в том числе в составе комиссии, на них распространяются права, предусмотренные пунктом 39 настоящего Положения, и они несут ответственность в соответствии с пунктом 40 настоящего Положения.

V. Обязанности руководителя и работников проверяемых подразделений

42. Руководитель проверяемого подразделения:

информирует работников подразделения о цели и характере проверки;

определяет работников подразделения для работы с членами комиссии;

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

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

содействовать комиссии в проведении проверки;

обеспечивать беспрепятственный доступ членов комиссии в служебные помещения проверяемого подразделения;

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

демонстрировать членам комиссии свою работу на автоматизированных рабочих местах в информационных системах, используемых при обработке персональных данных, включая выборку необходимой информации;

представлять членам комиссии документы (сведения), необходимые для проведения проверки, в сроки, установленные председателем комиссии.

44. В случае отсутствия документов (сведений), необходимых для проведения проверки, и (или) возникновения обстоятельств, препятствующих их представлению, руководитель проверяемого подразделения представляет председателю комиссии письменное объяснение с указанием причин невозможности представления запрашиваемых документов (сведений).

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

45. По результатам проведения проверки соблюдения режима защиты персональных данных составляется акт (при необходимости – в двух экземплярах) по форме согласно приложению № 7:

для проверок, проводимых Департаментом, – на общем бланке ОАО «РЖД» с продольным расположением реквизитов;

для проверок, проводимых подразделениями ОАО «РЖД» и региональными подразделениями, – на стандартных листах бумаги формата А4 (не на бланке).

Сведения о проверке отражаются в журнале учета проверок соблюдения режима защиты персональных данных по форме согласно приложению № 8 как в проверяемом подразделении, так и в подразделении, проводившем проверку.

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

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

о выявленных нарушениях режима защиты персональных данных с указанием соответствующих пунктов нормативных документов ОАО «РЖД»;

об устраненных на дату завершения проверки нарушениях.

47. Заключительная часть акта проверки содержит выводы комиссии о соблюдении режима защиты персональных данных в проверяемом подразделении и сведения о выявленных нарушениях режима защиты персональных данных. Документы, подтверждающие выявленные в ходе проверки нарушения режима защиты персональных данных, при необходимости приобщаются к акту.

48. 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 и пр.) председатель комиссии делает в акте соответствующую отметку.

49. Результаты проверки (акт проверки) председатель комиссии в установленном порядке представляет руководителю своего подразделения.

50. Акт проверки подлежит регистрации в Единой автоматизированной системе документооборота ОАО «РЖД» (далее – ЕАСД). В карточке документа проставляется отметка «Ограниченный доступ».

Акт проверки направляется в подразделение, в котором проводилась проверка, посредством ЕАСД с сопроводительным письмом. К карточке письма прикрепляется файл, содержащий отсканированную копию зарегистрированного акта проверки. При этом в карточке документа проставляется отметка «Ограниченный доступ».

51. Руководитель или ответственный за организацию обработки персональных данных в подразделении ОАО «РЖД» (региональном

подразделении), в котором проводилась проверка, не позднее 10 рабочих дней с даты получения акта проверки рассматривает его и утверждает план устранения нарушений, выявленных в ходе проверки соблюдения режима защиты персональных данных, по форме согласно приложению № 9. План регистрируется в ЕАСД и направляется в подразделение, проводившее проверку.

Датой получения акта проверки считается дата его поступления в ЕАСД.

52. Мероприятия, предусмотренные планом устранения нарушений, не влекущие за собой дополнительного финансирования и не требующие согласования с соответствующими подразделениями ОАО «РЖД», должны быть исполнены подразделением ОАО «РЖД» (региональным подразделением), в котором проводилась проверка, в течение одного месяца с даты получения акта проверки.

53. Отчет подразделения ОАО «РЖД» (регионального подразделения), в котором проводилась проверка, об исполнении плана устранения нарушений направляется в подразделение, проводившее проверку, не позднее 5 рабочих дней со дня истечения срока, предусмотренного указанным планом.

54. Материалы проверки (акт, план мероприятий, отчет об исполнении плана устранения нарушений и т.п.) приобщаются в соответствующие дела.

Дела с материалами проверок и журнал учета проверок соблюдения режима защиты персональных данных подлежат включению в утверждаемую номенклатуру дел.

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

55. Ответственные за организацию обработки персональных данных в подразделениях ОАО «РЖД» и региональных подразделениях:

обобщают и анализируют результаты контроля за соблюдением режима защиты персональных данных за первое полугодие и год;

формируют по результатам анализа статистический отчет о контроле за соблюдением режима защиты персональных данных, пояснительную записку к нему, составленные по форме согласно приложению № 10, а также аналитическую справку (далее – отчетные документы).

56. В аналитическую справку включается следующая информация:

отчет о результатах мониторинга согласно пункту 15 настоящего Положения и проведенных плановых, внеплановых и контрольных проверках;

сведения о выявленных в ходе мониторинга или проверок нарушениях требований законодательства Российской Федерации и нормативных документов ОАО «РЖД» в области персональных данных;

анализ причин и условий, способствовавших совершению нарушений режима защиты персональных данных;

сведения о мерах, принятых для устранения и недопущения выявленных нарушений режима защиты персональных данных;

отчет о выполнении полученных в отчетный период указаний руководства ОАО «РЖД» о принятии мер по обеспечению безопасности персональных данных;

информация о результатах проведенных контрольными (надзорными) органами государственной власти проверок;

выводы о соблюдении режима защиты персональных данных в подготовившем отчет подразделении.

Кроме того, аналитическая справка может содержать предложения о совершенствовании режима защиты персональных данных и повышении уровня их защищенности как в подготовившем отчет подразделении, так и в ОАО «РЖД» в целом.

57. Региональные подразделения направляют отчетные документы за первое полугодие и по итогам года в адрес подразделений ОАО «РЖД», в состав которых они входят или в ведении которых они находятся, в сроки, установленные пунктом 59 настоящего Положения.

58. Ответственные за организацию обработки персональных данных в филиалах и структурных подразделениях ОАО «РЖД» включают полученные от региональных подразделений сведения в состав своих отчетных документов.

59. Подразделения ОАО «РЖД» направляют в Департамент отчетные документы:

по итогам первого полугодия – до 15 июля текущего года;

по итогам года – до 15 января года, следующего за отчетным.

60. Сведения о проверках, проведенных в региональных подразделениях согласно плану проверок комитета РОК, включаются в отчетные документы железной дороги.

61. По итогам обобщения отчетных документов Департамент информирует ответственного за организацию обработки персональных данных в ОАО «РЖД» о состоянии режима защиты персональных данных в ОАО «РЖД» и вносит предложения по предупреждению возникновения и минимизации рисков, связанных с нарушениями режима защиты персональных данных.

Приложение № 1

к Положению о контроле
за соблюдением режима защиты
персональных данных
в ОАО «РЖД

УТВЕРЖДАЮ

_____
(руководитель подразделения ОАО «РЖД»/
регионального подразделения)
_____ И.О.Фамилия

«___»_____ 20___ г.

ПЛАН

проведения проверок соблюдения режима защиты персональных данных

в _____ в 20__ году

(наименование подразделения ОАО «РЖД» (регионального подразделения))

№ п/п	Наименование проверяемого подразделения	Адрес объекта проверки	Основание проверки	Период проведения проверки		Принимающие участие в проведении проверки подразделения ОАО «РЖД», хозяйственные общества с участием ОАО «РЖД», юридические лица, индивидуальные предприниматели	Форма проведения проверки (документарная, выездная, документарная и выездная)
				Дата начала проверки	Срок проведения проверки		

Ответственный за организацию
обработки персональных данных
(подразделения «ОАО «РЖД»/регионального подразделения) _____/_ _____
(подпись) (расшифровка подписи)

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 проверяемого подразделения	Адрес объекта проверки	Основание проверки	Период проведения проверки		Принимающие участие в проведении проверки подразделения ОАО «РЖД», хозяйственные общества с участием ОАО «РЖД», юридические лица, индивидуальные предприниматели	Форма проведения проверки (документарная, выездная, документарная и выездная)
				Дата начала проверки	Срок проведения проверки		
1							

Директор ОАО «РЖД» –
начальник Департамента
управления информационной
безопасностью

И.О.Фамилия

Приложение № 3

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

ПРИКАЗ
(оформляется на бланке
подразделения ОАО «РЖД»/
регионального подразделения)

Об образовании комиссии
по проведению проверки соблюдения режима защиты персональных данных в _____
(наименование проверяемого подразделения)

В соответствии с Положением о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от __ _____ 20__ г. № _____, (далее – Положение), приказываю:

1. Образовать комиссию по проведению проверки соблюдения режима защиты персональных данных в _____ в составе:
(наименование проверяемого подразделения)

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».

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

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. № ____, и_____
(основание для проведения проверки)

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 проверяемого подразделения)

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»

ПРЕДПИСАНИЕ
о проведении проверки
(оформляется на бланке
подразделения «ОАО «РЖД»/
регионального подразделения)

В соответствии с Положением о контроле за соблюдением режима защиты персональных данных в ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от _____ 20__ г. № ____, 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 проверяемого
_____.
подразделения)

Вопросы, рассматриваемые в ходе проверки:

_____.

Предписание действительно с _____ до _____ 20___ г.

Руководитель_____ И.О.Фамилия
(наименование 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»

УВЕДОМЛЕНИЕ
(оформляется на бланке
подразделения ОАО «РЖД»/
регионального подразделения)

Начальнику _____
(наименование проверяемого подразделения)

О проведении проверки

Уважаемый _____!

Сообщаем, что в соответствии с _____
(основание для проведения проверки)
будет проводиться проверка соблюдения режима защиты персональных данных в _____.
(наименование проверяемого 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 рассмотрению в ходе проверки, на __ л.

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

Приложение № 7

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

Экз.№_____

ОТКРЫТОЕ 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)

Настоящий акт составлен по результатам проверки соблюдения режима защиты персональных данных в

_____,
(наименование проверяемого подразделения)

проведенной на основании _____.
комиссией в составе:

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

Фамилия И.О. – _____
(должность)

Фамилия И.О. – _____
(должность)

В ходе проверки рассмотрены следующие вопросы:

_____
(основная часть согласно п.45 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 объекта проверки	Номер и дата предписания о проведении проверки	Подразделение (контрольный (надзорный) орган) проводившее проверку	Регистрационный номер акта проверки	Регистрационный номер плана устранения нарушений	Номер дела, где хранятся материалы проверки

Приложение № 9

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

УТВЕРЖДАЮ

_____

(должность руководителя
подразделения ОАО «РЖД»)

_____ _____

(подпись) (Ф.И.О.)

«___» _____ 20___г.

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

в_____

(наименование проверяемого подразделения)

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

Ответственный за организацию
обработки персональных данных _____/_____

(подпись) (расшифровка подписи)

«___» _____20__г.

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 контрольными (надзорными) органами:	
1.1.	Роскомнадзор	
1.2.	ФСБ России	
1.3.	ФСТЭК России	
1.4.	Прокуратура Российской Федерации	
1.5.	Иные контрольные (надзорные) органы	
2.	Получено предписаний об устранении нарушений, выявленных контрольными (надзорными) органами:	
2.1.	Роскомнадзор	
2.2.	ФСБ России	
2.3.	ФСТЭК России	
2.4.	Прокуратура Российской Федерации	
2.5.	Иные контрольные (надзорные) органы	
3.	Получено протоколов об административных правонарушениях от контрольных (надзорных) органов:	
3.1.	Роскомнадзор	
3.2.	ФСБ России	
3.3.	ФСТЭК России	

3.4.	Прокуратура Российской Федерации	
3.5.	Иные контрольные (надзорные) органы	
4.	Рассмотрено обращений (запросов) субъектов персональных данных или Роскомнадзора о нарушениях требований по обработке и обеспечению безопасности персональных данных	
5.	Проведено внутренних проверок	
6.	Выявлено нарушений режима защиты персональных данных	
7.	Проведено служебных расследований:	
7.1.	по фактам утраты материальных носителей персональных данных	
7.2.	по фактам распространения персональных данных	
7.3.	по фактам нарушения установленных требований при передаче персональных данных в электронном виде	
7.4	по иным фактам нарушения режима защиты персональных данных	
8.	Привлечено к дисциплинарной/материальной ответственности	
9.	Направлено обращений в правоохранительные органы в отношении лиц, допустивших нарушение режима защиты персональных данных	
10.	Заключено договоров с третьими лицами на обработку персональных данных (договоров поручения на обработку персональных данных)	
11.	Количество фактов трансграничной передачи персональных данных[1]	

Ответственный за организацию
обработки персональных данных _____/_____
(подпись) (расшифровка подписи)

«___» _____20__г.

[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 требуется. В случае если по всем пунктам статистического отчета сведения о контроле за соблюдением режима защиты персональных данных отсутствуют, пояснительная записка не составляется.

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 – 1.5 – указываются вид проверок, их сроки, мероприятия по контролю за соблюдением режима защиты персональных данных, проведенные в ходе проверок, сведения об отсутствии или наличии нарушений с наименованием вида нарушения и пунктов нормативных правовых актов Российской Федерации или нормативных документов ОАО «РЖД» по которым выявлены нарушения. Проверки, проведенные Департаментом, комиссией комитета РОК или подразделениями ОАО «РЖД» в подчиненных им региональных подразделениях (дирекциях, центрах и др.), расположенных в границах железных дорог, не учитываются;

по подпунктам 2.1 – 2.5 – перечисляются полученные предписания об устранении выявленных нарушений, включая сведения о нарушениях и сроках их устранения;

по подпунктам 3.1 – 3.5 – 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 – излагается суть рассмотренных обращений (запросов) субъектов персональных данных или Роскомнадзора о нарушениях требований по обработке и обеспечению безопасности персональных данных, результаты проведенных в подразделении проверок (подтвердилась или нет информация о нарушении);

по пункту 5 – перечисляются проведенные проверки с указанием их вида и результатов;

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 персональных данных;

по подпунктам 7.1 – 7.4 – указываются сведения, содержащиеся в заключении о результатах проведенных служебных расследований;

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, направленных по инициативе руководителя подразделения ОАО «РЖД» (регионального подразделения), в правоохранительные и контролирующие органы, в отношении лиц, допустивших нарушение режима защиты персональных данных, с указанием принятых по ним решений;

по пункту 10 – указываются реквизиты договоров, заключенных с третьими лицами на обработку персональных данных (предметом договора должна являться обработка персональных данных работников ОАО «РЖД» и других субъектов персональных данных);

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

Ответственный за организацию
обработки персональных данных _____/_____
(подпись) (расшифровка подписи)

«___» _____20__г.

Приложение № 1
к распоряжению ОАО «РЖД»
от « 7 »марта 2024 г. № 615/р

ПЕРЕЧЕНЬ
хозяйственных обществ с участием ОАО «РЖД»

1. АО «АК «ЖДЯ».
2. АО «Арена-2000».
3. АО «ВВРЗ им. С.М. Кирова».
4. АО «ВНИИЖТ».
5. АО «ВНИКТИ».
6. АО «ВРК-1».
7. АО «ВСМ».
8. АО «ДЦВ ВСЖД».
9. АО «ДЦВ ОЖД».
10. АО «ЖСИ».
11. АО «Желдорреммаш».
12. АО «Желдоручет».
13. АО «ЖТК».
14. АО «ЗСТ».
15. АО «Издательский дом «Гудок».
16. АО «ИМЗ».
17. АО «ИЦ ЖТ».
18. АО «ИЭРТ».
19. АО «Компания ТрансТелеКом».
20. АО «Люблинский ЛМЗ».
21. АО «Московский ЛРЗ».
22. АО «НИИАС».
23. АО «НПФ «БЛАГОСОСТОЯНИЕ».
24. АО «ОТЛК ЕРА».
25. АО «ОТЛК Логистика».
26. АО «ОТЛК Финансы».
27. АО «ОТЛК».
28. АО «ПНК».
29. АО «ПУЛ транс».
30. АО «РЖД Бизнес Актив».
31. АО «РЖД Логистика».
32. АО «РЖД Медицина».
33. АО «РЖД Управление активами».
34. АО «РЖД-инфраструктурные проекты».

35. АО «РЖДстрой».
36. АО «Росжелдорпроект».
37. АО «РПМ».
38. АО «РТА».
39. АО «Скоростные магистрали».
40. АО «ТВС».
41. АО «ТД РЖД».
42. АО «ТрансТех».
43. АО «УК «МТУ».
44. АО «ФГК».
45. АО «ФК «ЛОКОМОТИВ».
46. АО «ФПК».
47. АО «ЭКЗА».
48. АО «Экспериментальный завод «Металлист – Ремпутьмаш».
49. ОАО «ЭЛТЕЗА».
50. ООО «ЭНЕРГОПРОМСБЫТ».
51. АО «ЯЖДК».
52. ЗАО «ЮКЖД».
53. ООО «1520 (Сигнал)».
54. ООО «Аэроэкспресс».
55. ООО «ВСМ-Сервис».
56. ООО «ОП «РЖД-ОХРАНА».
57. ООО «РЖД Интернешнл».
58. ООО «РЖД Терминал».
59. ООО «РЖД-Технологии».
60. ООО «ТЛЦ «Белый Раст».

Приложение № 2
к распоряжению ОАО «РЖД»
от «7» марта 2024 г. № 615/р

ПЕРЕЧЕНЬ
пригородных пассажирских компаний – хозяйственных обществ с участием ОАО «РЖД»

1. АО «Алтай-Пригород».
2. АО «Байкальская ППК».
3. АО «Башкортостанская ППК».
4. АО «ВВППК».
5. АО «ВТП».
6. АО «ЗППК».
7. АО «КППК».
8. АО «Краспригород».
9. АО «Кубань Экспресс-Пригород».
10. АО «Кузбасс-пригород».
11. АО «МТ ППК».
12. АО «Омск-пригород».
13. АО «ПКС».
14. АО «ППК «Черноземье».
15. АО «ППК».
16. АО «Самарская ППК».
17. АО «Саратовская ППК».
18. АО «СЗППК».
19. АО «СКППК».
20. АО «Содружество».
21. АО «СПК».
22. АО «СППК».
23. АО «Экспресс Приморья».
24. АО «Экспресс-пригород».