УТВЕРЖДАЮ:
Заведующий
«Детский сад №251 ОАО «РЖД»
_____ Н.Ю.Тарасова
«__01__» ____апреля____ 2016 г.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги»

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее-Правила) в частном дошкольном образовательном учреждении детский сад № 251 ОАО «РЖД» (далее-Учреждение) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства российской Федерации в сфере персональных данных (далее ПДн): основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21.03.2012г. № 211.

1.3. Для обработки ПДн, необходимых для предоставления услуг Учреждения, воспитанникам, родителям (законным представителям), используется информационная система (далее – ИСПДн) ЕКАСУТР, предназначенная для осуществления деятельности в Учреждении, согласно утвержденному перечню ПДн.

1.4. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в частном дошкольном образовательном учреждении «Детский сад № 251 ОАО «РЖД» в соответствии с Трудовым кодексом российской федерации, используется информационная система ЕКАСУТР «Личные карточки», НПФ «Благосостояние» для передачи отчетности в ИНФС и ПФ.

1.5. Пользователями ИСПДн (далее – Пользователь) являются сотрудники по должностям «заведующий», «Делопроизводитель», «Старший воспитатель», «Главный бухгалтер», «Бухгалтер», участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющие доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги» проводятся в следующих целях:

1.6.1 проверка выполнения требований организационно-распорядительной документации по защите информации в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги» и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.6.2 оценка уровня осведомленности и знаний работников в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги» в области обработки и защиты персональных данных;

1.6.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Основанием для проведения внутреннего контроля являются требования Федерального закона № 152-ФЗ (часть 1, статья 18.1) и постановления Правительства Российской Федерации № 1119 (п. 17).

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги» разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся ответственным периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги».

2.3. Плановые контрольные мероприятия проводятся совместно с постоянной комиссией периодически в соответствии с утвержденным Планом

проведения контрольных мероприятий (далее – План) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги».

2.3.1. Внутренний контроль осуществляется путем проведения проверок в соответствии с планом внутренних проверок состояния защиты персональных данных.

2.3.2. Проверку проводит Комиссия, назначенная приказом заведующего

Учреждением, или на договорной основе юридическое лицо (индивидуальный предприниматель), имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2.3.3. Состав Комиссии не менее 3-х человек, включая лицо, ответственное за организацию обработки персональных данных. Все члены комиссии при принятии решения обладают равными правами.

2.3.4. Комиссия при проведении проверки обязана:

– провести анализ реализации мер, направленных на обеспечение выполнения

Оператором обязанностей, предусмотренных Федеральным законом № 152-ФЗ (статья 218.1, статья 19) и принятыми в соответствии с ним локальными актами Оператора определяющих его политику в отношении обработки персональных данных;

– провести анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства № 1119;

– провести анализ реализации Оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы;

– своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации;

– при проведении проверки соблюдать законодательство Российской Федерации, права и законные интересы Оператора.

2.3.4. Комиссия при проведении проверки вправе:

– запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

– получать доступ к информационным системам персональных данных в части касающейся ее полномочий;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;

– вносить директору Организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации.

2.3.5. При проведении проверки члены Комиссии не вправе:

– требовать представления документов и сведений, не относящихся к предмету проверки;

– распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

2.3.6. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и представляется руководителю организации для принятия соответствующего решения.

2.3.7. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

2.3.8. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных и политике оператора в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению руководителя Учреждением;

2.4.4 по решению Учредителя.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета проверок соблюдения режима защиты персональных данных.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение руководителю Учреждением.

4.4. Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета проверок соблюдения режима защиты персональных данных..

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий может привлекаться комиссия по информационной безопасности, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в частном дошкольном образовательном учреждении «Детский сад № 37 открытого акционерного общества «Российские железные дороги».

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех лиц, причастных к обработке персональных данных и допущенных к персональным данным работников, воспитанников, родителей (законных представителей), в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение ответственными инструкций и регламентов по обеспечению безопасности информации в частном дошкольном образовательном учреждении «Детский сад № 251 открытого акционерного общества «Российские железные дороги».
- Соблюдение Порядка доступа в помещения Учреждения, где ведется обработка персональных данных.
- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.
- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в Учреждении.
- Порядок и условия применения средств защиты информации.
- Состояние учета съемных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

Приложение 1

ПРОТОКОЛ № _____

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в частном дошкольном образовательном учреждении

«Детский сад № 251 ОАО «РЖД»

Настоящий Протокол составлен в том, что «__»_____201_ г.

_____ (комиссией)

(должность, Ф.И.О. сотрудника)

проведена проверка _____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

_____

(название документа)

_____

В ходе проверки проверено:

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____

Срок устранения нарушений: _____

Председатель комиссии:

фамилия и инициалы / подпись / должность

Члены комиссии:

фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность