

УТВЕРЖДЕНЫ
приказом АНО ДПО «Корпоративный
университет РЖД»
от «07» июня 2023 г. № КУ-47

ПРАВИЛА
АНО ДПО «Корпоративный университет РЖД»
«Осуществления внутреннего контроля соответствия обработки
персональных данных в структурных подразделениях
требованиям к защите персональных данных»

г. Москва, г. Щербинка
2023 г.



Версии документа

Версия	Дата изменения	Описание изменения	Автор изменения	Подпись
1	30.05.2019	Создание первой версии документа	Ефимова Т.С.	
2	08.06.2023	Актуализация документа	Винокурова Е.Н.	



Оглавление

1. Назначение документа	4
2. Термины и определения	4
3. Общие положения	4
4. Порядок осуществления внутреннего контроля	5
5. Ссылки на нормативные документы	7
Приложение № 1.....	8



1. Назначение документа

1.1. Настоящие правила (далее - Правила) устанавливают основания и порядок осуществления внутреннего контроля соответствия обработки персональных данных в структурных подразделениях АНО ДПО «Корпоративный университет РЖД» требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), а также принятыми в соответствии с ним правовыми актами. Правила определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

2. Термины и определения

Термин/сокращение	Определение/расшифровка
Персональные данные (Пдн)	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники
КУ/Корпоративный университет	АНО ДПО «Корпоративный университет «РЖД»

3. Общие положения

3.1. Настоящие Правила разработаны в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и принятыми в соответствии с ними правовыми актами.

3.2. Целью осуществления контроля является оценка общего состояния выполнения в процессах Корпоративного университета требований по обработке и защите Пдн, закрепленных законодательно и в локальных нормативных актах КУ.

3.3. При осуществлении внутреннего контроля соответствия обработки



персональных данных требованиям законодательства (далее - контроль) оценивается:

- наличие угрозы безопасности персональных данных при их обработке;
- выполнение организационных и технических мер по обеспечению безопасности персональных данных при их обработке; правомерность доступа к персональным данным;
- выполнение решений по предотвращению несанкционированного доступа к персональным данным с применением организационных и технических мер;
- выполнение правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.
- и пр.

3.4. Осуществление внутреннего контроля соответствия обработки персональных данных в структурных подразделениях, установленным требованиям, проводится в порядке, установленном настоящими Правилами.

4. Порядок осуществления внутреннего контроля

4.1. В Корпоративном университете установлены следующие виды контроля:

- текущий;
- периодический;
- внеплановый.

4.2. Текущий контроль организуют и проводят руководители структурных подразделений на постоянной основе.

Руководители структурных подразделений, ответственные за организацию обработки ПДн на местах, осуществляют контроль и постоянный мониторинг в области обработки и обеспечения безопасности персональных данных в своем структурном подразделении на основе анализа бизнес-процессов подразделения, риск-ориентированного подхода и с учетом накопленного опыта.

4.2.1. Проверку руководители осуществляют в соответствии с рекомендуемым типовым перечнем контрольных параметров, определенном в Приложении 1 к настоящим Правилам.

4.2.2. Используя типовой перечень контрольных параметров, руководитель структурного подразделения разрабатывает регламент проведения текущего контроля (чек-лист), отражающий следующие показатели:

- должностное лицо и его функции в части обработки ПДн;
- контролируемые показатели (осуществляемые действия);
- периодичность контроля;
- форма регистрации;
- действия при выявлении нарушений.

4.2.3. Текущий контроль осуществляется непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных.

4.3. Периодический контроль осуществляется группой уполномоченных лиц (Комиссией), назначенных приказом директора,

4.3.1. Периодический контроль может осуществляться как на рабочих



местах исполнителей, участвующих в ⁶ обработке персональных данных, так и путем направления запросов и рассмотрения документов для осуществления внутреннего контроля.

4.3.2. Периодический контроль предусматривает оценку Комиссией достаточности и эффективности мероприятий по организационному и техническому обеспечению безопасности персональных данных при их обработке.

4.3.3. Результаты проведения периодического контроля фиксируются в журнале проведения проверок с одновременным предоставлением руководителю Корпоративного университета отчета о проведении проверки, содержащем перечень нарушений (при их наличии), выявленных в ходе проверки.

4.4. Организация и проведение внепланового контроля может проводиться в случае:

- поступления жалоб от субъекта персональных данных на нарушение
- его прав в части обработки персональных данных;
- в результате выявления фактов незаконного распространения, разглашения персональных данных и прочих выявленных фактах нарушений требований законодательства в области защиты персональных данных;
- поступления служебной записки руководителю КУ от ответственных за обеспечение безопасности персональных данных в КУ лиц.

4.4.1. Решение о проведении внепланового контроля принимает руководитель Корпоративного университета.

4.4.2. Внеплановый контроль организуется и проводится уполномоченным лицом, назначенным приказом руководителя КУ, в порядке, установленном настоящими Правилами.

5. Ссылки на нормативные документы

5.1. Настоящие Правила подготовлены с учетом следующей нормативно-правовой и внутренней регламентирующей документации:

[1] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. 31.12.2017) «О персональных данных»;

[2] Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[3] Постановление Правительства РФ 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

[4] Организационное положение АНО ДПО «Корпоративный университет РЖД» «ОП_31 Политика по защите и обработке персональных данных в АНО ДПО «Корпоративный университет РЖД»;

[5] Организационное положение АНО ДПО «Корпоративный университет РЖД» «ОП_7 Положение о порядке хранения, защиты и работы с персональными данными в АНО ДПО «Корпоративный университет РЖД».



Приложение № 1

к Правилам «Осуществления внутреннего контроля соответствия обработки персональных данных в структурных подразделениях требованиям к защите персональных данных»

ПЕРЕЧЕНЬ

контрольных параметров проверок в области обработки и обеспечения безопасности персональных данных

Контрольные параметры и объекты проверок
Наличие законных целей и оснований обработки всех категорий персональных данных (документов, определяющих основания обработки персональных данных в КУ/структурном подразделении КУ)
Соответствие установленного перечня персональных данных по каждой категории субъекта ПДн фактически обрабатываемым в КУ
Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников, в том числе наличие утвержденных списков должностных лиц структурных подразделений, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей
Утвержденные перечни информационных систем персональных данных, эксплуатируемых в структурных подразделениях
Выборочные проверки сотрудников на предмет знания локальных нормативных актов и законодательства в области обработки и обеспечения безопасности персональных данных
Подтверждение факта ознакомления с локальными актами в области обработки и обеспечения безопасности персональных данных
Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
Наличие законных оснований передачи персональных данных третьим лицам
Соблюдение сроков хранения и порядка уничтожения персональных данных
Соблюдение процедур подготовки ответов на обращения субъектов персональных данных (при их наличии)
Своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в структурных подразделениях КУ, в связи с достижением целей обработки или потери необходимости в достижении этих целей
Условия хранения и состояние учета машинных носителей персональных данных
Соблюдение требований к паролям доступа
Отсутствие неправомерно размещенных персональных данных слушателей или работников в помещениях КУ или на официальном сайте







[The main body of the page contains extremely faint and illegible text, likely bleed-through from the reverse side of the paper. The text is too light to be transcribed accurately.]





Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

	Организация, сотрудник	Доверенность: рег. номер, период действия и статус	Сертификат: серийный номер, период действия	Дата и время подписания
Подписи отправителя:	 АНО ДПО "КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ РЖД" Баскин Роман Валерьевич, ДИРЕКТОР	 Не требуется для подписания	0135B49500C8AF9FBB4073E5B2 42B53DE9 с 17.03.2023 11:55 по 17.06.2024 11:55 GMT+03:00	07.05.2024 17:28 GMT+03:00 Подпись соответствует файлу документа
Подписи получателя:	 АНО ДПО "КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ РЖД" Баскин Роман Валерьевич, ДИРЕКТОР	 Не требуется для подписания	0135B49500C8AF9FBB4073E5B2 42B53DE9 с 17.03.2023 11:55 по 17.06.2024 11:55 GMT+03:00	07.05.2024 17:29 GMT+03:00 Подпись соответствует файлу документа