УТВЕРЖДЕНО:
Приказом Директора
ОАНО «ЧШК «СНЕГИРИ»
от «01» сентября 2022 года № 5-09/22

ПОЛОЖЕНИЕ

о защите персональных данных

СНЕГИРИ
частная школа

2022

Оглавление

1.Общие положения

1.1. Настоящее Положение о защите персональных данных (далее – «Положение») разработано в соответствии со ст. 18.1 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «Закон о персональных данных»), Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными актами Российской Федерации, и определяет меры защиты персональных данных, устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.2. Положение действует в отношении всех персональных данных, которые обрабатывает Общеобразовательная автономная некоммерческая организация «ЧАСТНАЯ ШКОЛА «СНЕГИРИ» и распространяется на отношения в области обработки и защиты персональных данных, возникшие как до, так и после утверждения настоящего Положения.

1.3. Мероприятия по защите персональных данных осуществляются за счет средств Оператора.

1.4. В Положении используются следующие термины (понятия):

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

1.4.2.Специальные категории персональных данных – информация, касающееся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

1.4.3.Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

1.4.4.Оператор – Общеобразовательная автономная некоммерческая организация «ЧАСТНАЯ ШКОЛА «СНЕГИРИ» (ОГРН 1207700098297; адрес места нахождения: 119285, г. Москва, ул. Минская, д. 2В, корп. 2, пом. 224), самостоятельно или совместно с другими лицами организующая и/или осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

1.4.6.Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких.

1.4.7.Автоматизированная обработка персональных данных – обработка

персональных данных с помощью средств вычислительной техники;

1.4.8.Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.4.9.Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

1.4.11.Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и/или в результате которых уничтожаются материальные носители персональных данных;

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

1.4.13.Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.Обязательные мероприятия по обеспечению безопасности персональных данных

2.1.Меры защиты персональных данных Оператора направлены на сохранение конфиденциальности персональных данных, исключение случаев неакционерного доступа к ним и совершения иных неправомерных действий с персональными данными.

2.2.Оператор принимает следующие меры по защите персональных данных:

2.2.1.Назначение приказом Директора лица, ответственного за организацию обработки персональных данных;

2.2.2.Назначение приказом Директора лица, ответственного за безопасность персональных данных (при необходимости);

2.2.3.Разработка локальных нормативных актов, регулирующих вопросы обработки и защиты персональных данных;

2.2.4.Установление правил доступа к персональным данным и регулярный пересмотр данных правил;

2.2.5.Определение перечня информационных ресурсов, содержащих персональные данные, и установление правил доступа к ним, регулярный пересмотр данного перечня и правил доступа;

2.2.6.Установление индивидуальных паролей доступа работников к информационным ресурсам, содержащим персональные данные, обеспечение сохранения данных паролей в специализированных инструментах, используемых работниками Оператора персонально;

2.2.7.Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

2.2.8.Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами, которое обеспечивает сканирование съемного носителя на предмет наличия вредоносного программного обеспечения в автоматическом режиме до его использования;

2.2.9.Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

2.2.10.Обнаружение фактов несанкционированного доступа к персональным данным;

2.2.11.Восстановление персональных данных, модифицированных и/или уничтоженных вследствие несанкционированного доступа к ним;

2.2.12.Использование инструмента резервного копирования данных на носитель, географически удаленный от Оператора, и регулярное тестирование резервных копий на предмет работоспособности не реже 2 раз в год (ручным и/или машинным способами);

2.2.13.Обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, и локальных нормативных актов, регулирующих вопросы обработки и защиты персональных данных;

2.2.14.Осуществление внутреннего контроля;

2.2.15.Определение типа угроз безопасности и уровней защищенности персональных данных.

3.Защита персональных данных на материальных носителях

3.1.Сохранность материальных носителей, содержащих персональные данные, и отсутствие неакционерного доступа к ним, обеспечивается Оператором путем раздельного хранения материальных носителей персональных данных в сейфах или и металлических шкафах в специальных защищаемых помещениях.

3.2.В отношении каждого такого помещения Оператором устанавливается особый режим доступа путем определения перечня лиц (должностей), имеющих к ним доступ.

Лица, не имеющие доступа к специальным защищаемым помещениям, не должны иметь возможности самостоятельного доступа в такие помещения без сопровождения.

Сопровождающий работник должен постоянно контролировать действия таких лиц в помещении.

Специальное защищаемое помещение в отсутствие работника, имеющего к нему доступ, должно быть закрыто на механический замок и/или электронный.

Такое помещение находится под сигнализацией, открываются и закрываются самим работником.

3.3.Оператором реализуется следующая процедура контроля и учета ключей:

–ключи и журнал учета ключей хранятся на посту охраны;

–ключи выдаются в соответствии со списками лиц, имеющих доступ в специальные защищаемые помещения, и под личную подпись;

–факт выдачи ключа фиксируется путем внесения записи в журнал сведений о

работнике, которому выданы ключи, дате и времени выдачи, а также отметки о сдаче ключей.

3.4.При работе с персональными данными на материальных носителях работник, допущенный к обработке таких данных, обязан: исключить возможность подсматривания информации посторонними лицами, в том числе и с помощью технических средств (стационарных и встроенных в мобильные телефоны фото- и видеокамер и т.п.); убирать все материальные носители, содержащие персональные данные, в сейф или металлический шкаф при покидании рабочего места в течение рабочего дня даже на небольшой период времени.

4.Защита персональных данных в информационных системах

4.1.В целях контроля за защищенностью персональных данных в информационных системах Оператор проводит инвентаризацию таких систем путем опроса работников на предмет наличия информационных ресурсов, в которых они обрабатывают персональные данные.

4.2.Перечень информационных ресурсов, содержащих персональные данные, разрабатывается Ответственным за обработку персональных данных по результатам опроса работников и после утверждается приказом Директором. Такой перечень подлежит пересмотру и при необходимости актуализации не реже одного раза в месяц.

4.3.Для всех эксплуатируемых информационных систем персональных данных Оператор определяет уровни защищенности персональных данных, исходя из следующих типов угроз:

4.3.1.Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе, то есть в системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель, и это потенциально может привести к неправомерному использованию персональных данных.

4.3.2.Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе, то есть потенциальные проблемы с прикладным программным обеспечением – внешними программами, которые установлены на компьютерах работников.

4.3.3.Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, то есть потенциальной опасности ни от системного, ни от программного обеспечения нет.

4.4.При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных:

4.4.1.Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

–для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся работниками Оператора.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах Оператор выполняет следующие требования:

–организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

–обеспечивает сохранность носителей персональных данных;

–утверждает документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

–использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

–назначает должностное лицо (работника), ответственное за обеспечение безопасности персональных данных в информационной системе.

–организует доступ к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

–обеспечивает автоматическую регистрацию в электронном журнале безопасности изменений полномочий работника Оператора по доступу к персональным данным, содержащимся в информационной системе;

–создает структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возлагает на одно из структурных подразделений функций по обеспечению такой безопасности.

4.4.2.Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

–для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных

данных работников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся работниками Оператора;

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся работниками Оператора;

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся работниками Оператора;

–для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся работниками Оператора.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах Оператор выполняет следующие требования:

–организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

–обеспечивает сохранность носителей персональных данных;

–утверждает документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

–использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

–назначает должностное лицо (работника), ответственное за обеспечение безопасности персональных данных в информационной системе.

–организует доступ к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

4.4.3.Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные работников Оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся работниками Оператора;

–для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных работников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся работниками Оператора;

–для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных работников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся работниками Оператора;

–для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

–для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся работниками Оператора.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах Оператор выполняет следующие требования:

–организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

–обеспечивает сохранность носителей персональных данных;

–утверждает документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

–использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

–назначает должностное лицо (работника), ответственное за обеспечение безопасности персональных данных в информационной системе.

4.4.4.Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

–для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

–для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных работников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся работниками Оператора.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах Оператор выполняет следующие требования:

–организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

–обеспечивает сохранность носителей персональных данных;

–утверждает документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

–использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

4.5.При автоматизированной обработке персональных данных работник, допущенный к обработке таких данных, обязан: сохранять логины и пароли от информационных систем в специализированных инструментах; исключить возможность подсматривания информации посторонними лицами, в том числе и с помощью технических средств (стационарных и встроенных в мобильные телефоны фото- и видеокамер и т.п.); блокировать компьютер при покидании рабочего места в течение рабочего дня даже на небольшой период времени.

5.Предотвращение и выявление нарушений законодательства РФ в области обработки и защиты персональных данных

5.1.Основным способом выявления нарушений законодательства РФ, действующего в области обработки и защиты персональных данных, и методом реагирования на нарушения установленного порядка обработки, является организация Оператором внутреннего контроля за процессом безопасности обработки персональных данных.

5.2.Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

– обеспечение соблюдения работниками Оператора требований Закона о персональных данных, настоящего Положения и иных локальных нормативных актов Оператора, регулирующих порядок обработки персональных данных;

– оценка компетентности работников Оператора, задействованных в обработке персональных данных;

– обеспечение работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности персональных данных;

– выявление нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений;

– принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки персональных данных, так и в работе технических средств информационных систем персональных данных;

– разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий;

– осуществление контроля исполнения рекомендаций и указаний по устранению нарушений.

5.3.Мероприятия по внутреннему контролю за обработкой и обеспечением безопасности персональных данных осуществляются в форме проверок на плановой основе, а также при необходимости внепланово.

Плановые проверки проводятся не реже одного раза в полугодие – в октябре и апреле на основании приказа Директора по списку контрольных вопросов, утвержденных приказом Роскомнадзора от 24.12.2021 № 253.

Решение о необходимости проведения внеплановых проверок принимает Ответственный за обеспечение безопасности персональных данных (при наличии такого лица у Оператора) либо Ответственный за организацию обработки персональных данных. Основанием для внеплановой проверки могут быть: возросшие риски информационной безопасности для обрабатываемых персональных данных, существенные изменения в среде обработки персональных данных и т.п.

Внеплановые проверки не заменяют плановые проверки и проводятся не реже одного раза в полугодие и включают в себя:

– проверку деятельности работников Оператора, допущенных к работе с персональными данными, на соответствие порядку обработки и обеспечения безопасности персональных данных, установленному настоящим Положением и Положением об обработке персональных данных;

– проверку работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных;

– проверку соответствия предоставленных прав доступа работников к персональным данным утвержденному Перечню должностей работников, допущенных к работе с персональными данными, а также Перечню информационных ресурсов, содержащих персональные данные;

– проверку минимальной длины и сложности паролей;

– проверку периодичности смены паролей;

– проверку рабочих мест на предмет отсутствия свободного доступа к материальным носителям, содержащих персональные данные;

– проверку отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения;

– мониторинг журналов протоколирования событий аутентификации.

5.4.Контрольные мероприятия (плановые/внеплановые проверки) организуются Ответственным за обеспечение безопасности персональных данных (при наличии такого лица у Оператора) либо Ответственный за организацию обработки персональных данных. В случае передачи части функций в области информационных технологий сторонним организациям указанные контрольные мероприятия осуществляют эти сторонние организации. Требования по осуществлению контрольных мероприятий указываются в договорах с этими сторонними организациями.

5.5.Результаты проверок оформляются актами. Выявленные в ходе проверок нарушения, а также отметки об их устранении фиксируются в журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности персональных данных. При необходимости лицо, осуществляющее контрольные мероприятия, предлагает меры по минимизации последствий выявленных угроз информационной безопасности.

5.6.В случае обращения субъекта персональных данных по поводу неправомерных действий с его персональными данными, а также при выявлении по результатам проверки нарушений, допущенных работниками при обработке или защите персональных данных, Оператор проводит внутреннее расследование.

Ответственный за обеспечение безопасности персональных данных (при наличии такого лица у Оператора) либо Ответственный за организацию обработки персональных данных проводит опрос очевидцев, подозреваемых лиц, предположительно допустивших нарушение.

В ходе проведения опроса выясняется:

– дата и время совершения нарушения;

– обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;

– последствия, возникшие вследствие совершения нарушения.

Все опрашиваемые лица должны предоставить объяснительные записки (подробные письменные показания с подписью опрашиваемого).

Ответственный за обеспечение безопасности персональных данных (при наличии такого лица у Оператора) либо Ответственный за организацию обработки персональных данных оценивает последствия, возникшие вследствие совершения нарушения.

После указанных действий и не позднее 24 часов с даты обращения субъекта персональных данных/ обнаружения нарушения Ответственный за обеспечение безопасности персональных данных (при наличии такого лица у Оператора) либо Ответственный за организацию обработки персональных данных уведомляет Роскомнадзор о следующих выясненных обстоятельствах:

– произошедшем нарушении (инциденте);

– предполагаемых причинах, повлекших нарушение прав субъектов персональных данных,

– предполагаемом вреде, нанесенном правам субъектов персональных данных,

– принятых мерах по устранению последствий соответствующего инцидента;

– лице, уполномоченном Оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом.

По итогам разбирательства Ответственный за обеспечение безопасности персональных данных (при наличии такого лица у Оператора) либо Ответственный за организацию обработки персональных данных составляет заключение, в котором должны быть приведены сведения:

– дата и время выявления нарушения (инцидента), в отношении которого проводилось разбирательство;

– предполагаемые причины, повлекшие нарушение прав субъектов персональных данных;

– характеристика персональных данных;

– предполагаемый вред, нанесённый правам субъектов персональных данных;

– принятые меры по устранению последствий нарушения (инцидента);

– сведения о лицах, действия которых стали причиной нарушения (инцидента) – при наличии;

– предложения по привлечению виновника к ответственности;

– иные дополнительные сведения, предоставляемые по желанию.

Заключение согласовывается Директором и после чего предоставляется в Роскомнадзор не позднее 72 часов с момента обнаружения нарушения (инцидента).

6.Устранение последствий нарушений законодательства РФ в области обработки и защиты персональных данных

6.1.В случае выявления у Оператора фактов нарушения действующего законодательства РФ при обработке и защите персональных данных, Оператор принимает меры по предотвращению таких нарушений, а также устранению (минимизации) последствий таких нарушений, в том числе, но не ограничиваясь:

–привлекает виновных лиц к ответственности;

–осуществляет уничтожение, обезличивание, исправление или блокирование персональных данных, в порядке и сроки, предусмотренные действующим законодательством РФ, Положением об обработке персональных данных;

–исходя из фактических обстоятельств допущенного нарушения, принимает дополнительные правовые, организационные и/или технические меры для предотвращения нарушений и устранения (минимизации) последствий таких нарушений;

–возмещает убытки и/или моральный вред, причиненные указанным нарушением;

–принимает иные доступные меры, исключающие в дальнейшем (сводящих к минимуму) вероятность повторения подобного нарушения, а также устраняющие последствия такого нарушения.

7. Заключительные положения

7.1.Настоящее Положение вступает в действие с даты ее утверждения Директором и подлежит обязательному опубликованию в информационно-телекоммуникационной сети «Интернет» на сайте Оператора в течение 10 дней.

7.2.Положение действует до момента его отмены Директором и утверждения нового Положения или изменения и/или дополнения к настоящему Положению.

В случае, если в результате изменения законодательства РФ отдельные пункты Положения вступят в противоречие с нормами законодательства РФ, эти пункты утрачивают силу, и до момента внесения изменений в настоящее Положение, следует руководствоваться законодательством РФ.

7.3.Контроль за исполнением требований настоящего Положения осуществляется уполномоченным лицом, ответственным за обеспечение безопасности персональных данных у Оператора.