

ПОЛИТИКА
бюджетного учреждения здравоохранения Удмуртской Республики
«Республиканский врачебно-физкультурный диспансер
Министерства здравоохранения Удмуртской Республики»
в отношении обработки персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика бюджетного учреждения здравоохранения Удмуртской Республики «Республиканский врачебно-физкультурный диспансер Министерства здравоохранения Удмуртской Республики» в отношении обработки персональных данных (далее – Политика) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Политика разработана с целью обеспечения в бюджетном учреждении здравоохранения Удмуртской Республики «Республиканский врачебно-физкультурный диспансер Министерства здравоохранения Удмуртской Республики» (далее – Диспансер, Оператор) защиты прав и свобод субъекта персональных данных при обработке его персональных данных.

1.3. Настоящей политикой определяются цели, способы и принципы обработки Оператором персональных данных, перечень персональных данных, обрабатываемых Оператором, обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами

несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Лицо, ответственное за организацию обработки персональных данных – лицо, назначенное Оператором.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

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

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

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.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор – Диспансер, т.е. юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

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

Согласие субъекта персональных данных на обработку его персональных данных – согласие в письменной форме субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Специальные персональные данные – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Субъект персональных данных – физическое лицо, обладающее определёнными персональными данными.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных необходима для оформления возникновения, изменения и прекращения трудовых и иных непосредственно связанных с ними отношений, или гражданско-правовых отношений, в том числе для:

- содействия работникам в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- прохождения обязательного периодического медицинского осмотра;
- оформления всех видов поощрений (награждений), дисциплинарных и иных взысканий в отношении субъекта персональных данных;
- подготовки документов по рассмотрению устных и письменных обращений субъекта персональных данных;
- ведения бухгалтерского и налогового учета, формирования, изготовления, составления и своевременной подачи всех видов отчетов и отчетности, установленных законодательством, а также по запросу компетентных органов;
- ведения индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования.

3.2. Обработка персональных данных необходима для осуществления Диспансером основной уставной деятельности, в том числе в соответствии с лицензионными требованиями, установленными законодательством.

3.3. Обработка персональных данных необходима для исполнения Диспансером действующего законодательства.

3.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем по которому является субъект персональных данных, а также заключения договора инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем.

3.5. Обработка персональных данных необходима для оказания первичной медико-санитарной и специализированной медицинской помощи населению.

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных осуществляется на законной и справедливой основе.

4.2. Обработка персональных данных ограничивается достижением конкретных, определенных в настоящей Политике законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.

4.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

4.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оператором подлежат обработке следующие персональные данные субъектов персональных данных:

1) персональные данные субъектов персональных данных – работники Диспансера:

- фамилия, имя, отчество, дата и место рождения;
- гражданство;
- национальность;
- пол;
- адрес места регистрации и (или) места фактического проживания, номер домашнего телефона, номер сотового телефона;
- данные паспорта гражданина Российской Федерации или иного документа, удостоверяющего личность;

- номер страхового свидетельства обязательного пенсионного страхования;

- номер полиса обязательного медицинского страхования;
- идентификационный номер налогоплательщика;
- образование (уровень образования, специальность (направление), наименование учебного заведения, его местонахождение, факультет (отделение), год поступления и окончания или ухода (в том числе с какого курса), № и серия диплома (удостоверения), наличие ученой степени, ученого звания, научных трудов и изобретений;

- владение иностранными языками;
- сведения о выполняемой работе с начала трудовой деятельности (месяц и год вступления и ухода, занимаемая должность, местонахождение учреждения, организации), занимаемой должности, переводах на иные должности и основании назначения (перевода), стаже работы;

- табельный номер;
- номер служебного телефона;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о дисциплинарных и иных взысканиях;
- сведения об аттестации (дата, решение комиссии, основание);
- сведения об оплате труда по замещаемой должности;
- номер лицевого счета в банке, вид банковской карты, наименование банка, номер филиала;

- сведения о пребывании за границей (время пребывания, страна, цель);
- сведения о воинском учете;
- сведения о социальных льготах;
- данные водительского удостоверения;
- сведения об исполнительных листах, в том числе фамилия, имя, отчество, банковские данные получателей выплат по исполнительным листам;

- данные о состоянии здоровья, времени нетрудоспособности, о страховом стаже, о суммах начисленных пособий по нетрудоспособности;

- сведения о близких родственниках;
- сведения о семейном положении, данные свидетельства о заключении (расторжении) брака;

- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами, Положением об обработке персональных данных в БУЗ УР «РВФД МЗ УР»;

2) персональные данные субъектов персональных данных – пациенты Диспансера:

- фамилия, имя, отчество, дата рождения;
- гражданство;
- пол;
- адрес места регистрации и (или) места фактического проживания, номер домашнего телефона, номер сотового телефона;

- данные паспорта гражданина Российской Федерации или иного документа, удостоверяющего личность;

- номер полиса обязательного медицинского страхования;
- сведения о состоянии здоровья;
- фамилия, имя, отчество представителя субъекта персональных данных;
- адрес места регистрации и (или) места фактического проживания представителя субъекта персональных данных,
- номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе,
- реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами, Положением об обработке персональных данных в БУЗ УР «РВФД МЗ УР».

5.2. Основанием для обработки персональных данных является согласие субъекта персональных данных на обработку его персональных данных.

5.3. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

5.4. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки персональных данных. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных осуществляется путем смешанной (автоматизированной и неавтоматизированной) обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, уничтожение); передача полученной в ходе обработки информации может осуществляться на бумажных и (или) магнитных носителях.

7. ПЕРЕЧЕНЬ МЕР, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

7.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2. Для обеспечения безопасности персональных данных Оператором принимаются следующие меры:

7.2.1. Использование парольной защиты для входа в информационную систему персональных данных;

7.2.2. Использование антивирусной защиты информационной системы персональных данных;

7.2.3. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

7.2.4. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным, немедленное доведение этой информации до руководства Диспансера и немедленное принятие мер, направленных на устранение выявленных фактов несанкционированного доступа;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- учет применяемых средств защиты информации, соблюдение эксплуатационной и технической документации к ним, носителей персональных данных;
- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

7.2.5. Организация хранения персональных данных, зафиксированных на материальных носителях, направленная на обеспечение безопасности персональных данных, в том числе:

- персональные данные субъектов персональных данных – пациенты Диспансера хранятся на бумажных носителях в изолированном, недоступном для неконтролируемого пребывания посторонних лиц помещении (регистратуре);
- персональные данные субъектов персональных данных – работники Диспансера хранятся в приспособленном для этой цели помещении, недоступном для неконтролируемого пребывания посторонних лиц, отдельно от других дел, личные дела уволенных работников Диспансера передаются в установленном порядке на хранение в архив Диспансера;
- помещения для хранения персональных данных на бумажных, материальных носителях оборудуются замками и системой охранной и пожарной сигнализаций;

7.2.6. Издание документов, определяющих политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, в том числе:

- издание политики в отношении обработки персональных данных;
- принятие положения об обработке персональных данных;

- определение перечня информационных систем персональных данных;
- разработка и издание обязательства о неразглашении информации, содержащей персональные данные, лицом, допущенным к обработке персональных данных;
- принятие правил рассмотрения запросов субъектов персональных данных или их представителей;

7.2.7. Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, а также выполнение работниками Оператора следующих требований:

- знание и строгое выполнение установленных правил обработки и защиты информации и соблюдение принятого режима безопасности персональных данных;
- поддержание режима безопасности персональных данных при выборе и использовании паролей;
- обеспечение надлежащей защиты оборудования от посторонних воздействий и несанкционированного доступа;
- запрет на самостоятельную установку постороннего программного обеспечения, подключение личных мобильных устройств и носителей информации, а также запись на них защищаемой информации;
- запрет на разглашение защищаемой информации, которая стала им известна при работе с информационными системами Диспансера, третьим лицам;

7.2.8. Назначение ответственного за организацию обработки персональных данных, определение его обязанностей и ответственности за нарушение законодательства о персональных данных, в том числе:

- осуществление внутреннего контроля за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников Диспансера положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработка обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;
- разработка организационных распорядительных документов по обеспечению безопасности персональных данных в Диспансере;
- организация повышения осведомленности руководства и работников Диспансера по вопросам обеспечения безопасности персональных данных.

8. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Субъект персональных данных имеет право на получение сведений,

указанных в пункте 8.2 настоящей Политики, за исключением случаев, предусмотренных законодательством Российской Федерации. Субъект персональных данных вправе требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые Оператором способы обработки персональных данных;
- 4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- 6) сроки обработки персональных данных, в том числе сроки их хранения;

- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», настоящей Политикой и положением об обработке персональных данных в Диспансере;

- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

- 10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

8.3. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и настоящей Политики или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

9. ОБЯЗАННОСТИ ОПЕРАТОРА

9.1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную пунктом 8.2 настоящей Политики.

9.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

9.3. Оператор обязан принимать правовые, организационные и технические меры, необходимые и достаточные для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

9.4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

9.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных.

10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1 Лица, виновные в нарушении требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», настоящей Политики несут предусмотренную законодательством Российской Федерации ответственность.