

УТВЕРЖДАЮ
Директор МБОУ СОШ №10
им. С.И. Холодова ст. Новощербиновская
Е.М. Пидварко
« ____ » _____ 2021г.

ПОЛОЖЕНИЕ об обработке и защите персональных данных

1. Общие положения

1.1. Настоящее Положение имеет своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Настоящее Положение об обработке и защите персональных данных (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников, обучающихся (воспитанников) в соответствии с законодательством Российской Федерации и гарантии конфиденциальности сведений о работнике предоставленных работником работодателю.

1.3. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 21.03.2012 N 211-ФЗ "О персональных данных", иными нормативно-правовыми актами, действующими на территории Российской Федерации.

2. Основные понятия

Для целей настоящего Положения используются следующие понятия:

2.1. **Оператор персональных данных** (далее оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. В рамках настоящего положения оператором является – МБОУ СОШ №10 им. С.И. Холодова ст. Новощербиновская»;

2.2. **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.

2.3. **Субъект** - субъект персональных данных.

2.4. **Работник** - физическое лицо, состоящее в трудовых отношениях с оператором.

2.5. **Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.6. **Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-

телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.7. **Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

2.9. **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.

2.10. К персональным данным относятся:

2.10.1. Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта.

2.10.2. Информация, содержащаяся в трудовой книжке работника.

2.10.3. Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования.

2.10.4. Сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу.

2.10.5. Сведения об образовании, квалификации или наличии специальных знаний или подготовки.

2.10.6. Сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации.

2.10.7. Сведения о семейном положении работника.

2.10.8. Информация медицинского характера, в случаях, предусмотренных законодательством.

2.10.9. Сведения о заработной плате работника.

2.10.10. Сведения о социальных льготах;

2.10.11. Сведения о наличии судимостей;

2.10.12. Место работы или учебы членов семьи;

2.10.13. Содержание трудового договора;

2.10.14. Подлинники и копии приказов по личному составу;

2.10.15. Основания к приказам по личному составу;

2.10.16. Документы, содержащие информацию по повышению квалификации и переподготовке сотрудника, его аттестация, служебное расследование.

2.10.17. Сведения о награждении государственными наградами

3. Обработка персональных данных

3.1. Общие требования при обработке персональных данных.

В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных обязаны соблюдаться следующие требования:

3.1.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов РФ и РД, содействия субъектам персональных данных в трудоустройстве, продвижении по службе, обучении, контроля количества и качества выполняемой работы, обеспечения личной безопасности субъекта персональных данных и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора.

3.1.2. Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

3.1.3. При принятии решений, затрагивающих интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.4. Работники или их законные представители должны быть ознакомлены под расписку с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

3.1.5. Субъекты персональных данных, не являющиеся работниками, или их законные представители имеют право ознакомиться с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

3.1.6. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

3.2. Получение персональных данных.

3.2.1. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку оператором.

3.2.2. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на их обработку оператором.

3.2.3. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

3.2.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случаях указанных в пункте 3.2.2 настоящего положения согласие может быть отозвано законным представителем субъекта персональных данных.

3.2.5. В случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится у оператора.

3.2.6. Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.

3.2.7. Запрещается получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.8. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

3.3. Хранение персональных данных.

3.3.1. Хранение персональных данных субъектов осуществляется кадровой службой, бухгалтерией, на бумажных и электронных носителях с ограниченным доступом.

3.3.2. Личные дела хранятся в бумажном виде в папках. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.

3.3.3. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно "Положению об особенностях обработки персональных данных. Осуществляемой без использования средств автоматизации", утвержденному постановлением правительства РФ 15 сентября 2008 г. N 687.

3.4. Передача персональных данных

3.4.1. При передаче персональных данных субъекта оператор обязан соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;

- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции;

- передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;

3.4.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.4.3. Внутренний доступ (доступ внутри организации) к персональным данным субъекта. Право доступа к персональным данным субъекта имеют:

- руководитель организации;

- бухгалтер;

- сотрудник кадровой службы;

- непосредственные руководители по направлению деятельности (доступ к персональным данным сотрудников, непосредственно находящихся в его подчинении);

- завуч (доступ к персональным данным субъектов в части его касающейся);

- классный руководитель (доступ к персональным данным учеников своего класса в части его касающейся);

- учитель (доступ к информации, содержащейся в классных журналах тех классов, в которых он ведет занятия;

- сам субъект, носитель данных.

3.4.4. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных.

3.4.5. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

3.4.6. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

3.5. Уничтожение персональных данных

3.5.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.5.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

4. Права и обязанности субъектов персональных данных и оператора

4.1. В целях обеспечения защиты персональных данных субъекты имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;

- при отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

- дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

- требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

- обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите персональных данных субъекта.

4.2. Для защиты персональных данных субъектов оператор обязан:

- за свой счет обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством РФ;

- ознакомить работника или его представителей с настоящим положением и его правами в области защиты персональных данных под расписку;

- по запросу ознакомить субъекта персональных данных, не являющегося работником, или в случае недееспособности либо несовершеннолетия субъекта, его законных представителей с настоящим положением и его правами в области защиты персональных данных;

- осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

- предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим положением и законодательством Российской Федерации;

- обеспечить субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

- по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

4.3. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности..

5. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

5.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

5.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

УТВЕРЖДАЮ
Директор МБОУ СОШ №10
им. С.И. Холодова ст. Новощербиновская
_____ Е.М. Пидварко

Типовой должностной регламент специалиста по обеспечению безопасности персональных данных

I. Общие положения

1.1. Настоящий должностной регламент специалиста по обеспечению безопасности персональных данных (далее - Регламент) определяет основные цели, функции и права специалиста по обеспечению безопасности персональных данных (далее - Специалист) в соответствующей организации.

1.2. Специалист назначается приказом (или иным документом) Руководителя организации на основании Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. N 912-51, во исполнение Федерального закона "О персональных данных" N 152-ФЗ от 27.07.2006 г.

1.3. Специалист проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

1.4. Непосредственное руководство работой специалиста осуществляет заместитель Руководителя организации, курирующий вопросы защиты информации.

Назначение и освобождение от должности специалиста производится Руководителем организации.

1.5. Специалист назначается из числа сотрудников соответствующей организации, имеющих опыт работы по основной деятельности соответствующей организации или в области защиты.

1.6. Специалист приравнивается по оплате труда, льготам и премированию к соответствующим категориям работников основных подразделений соответствующей организации.

1.7. Работа специалиста проводится в соответствии с планами работ, утверждаемыми непосредственным руководителем или руководителем организации.

1.8. В своей работе специалист руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами и указаниям Руководителя организации и другими руководящими документами по обеспечению безопасности персональных данных.

II. Основные функции специалиста

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в соответствующей организации.

2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию информационных систем персональных данных.

2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе

- мероприятия по размещению, охране, организации режима допуска в помещения, где ведется обработка персональных данных;

- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;

- мероприятия по защите от несанкционированного доступа к персональным данным

- мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование..

2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Постоянный контроль за обеспечением уровня защищенности персональных данных.

2.9. Участие в подготовке объектов соответствующей организации к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.10. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в соответствующей организации.

2.11. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.12. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в соответствующей организации.

2.13. Проведение периодического контроля эффективности мер защиты персональных данных в соответствующей организации. Учет и анализ результатов контроля.

2.14. Организация повышения осведомленности руководства и сотрудников в соответствующей организации по вопросам обеспечения безопасности персональных данных, сотрудников подведомственных предприятий, учреждений и организаций.

2.15. Подготовка отчетов о состоянии работ по обеспечения безопасности персональных данных в соответствующей организации.

III. Права специалиста

Специалист имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность структурных подразделений соответствующей организации в части выполнения ими требований по обеспечению безопасности персональных данных.

3.5. Вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.6. Привлекать в установленном порядке необходимых специалистов из числа сотрудников соответствующей организации для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

IV. Ответственность специалиста

4.1. Специалист несет персональную ответственность за:

правильность и объективность принимаемых решений;

правильное и своевременное выполнение приказов, распоряжений, указаний руководства соответствующей организации по вопросам, входящим в возложенные на него функции;

выполнение возложенных на него обязанностей, предусмотренных настоящим Регламентом;

соблюдение трудовой дисциплины, охраны труда;

качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.

согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

УТВЕРЖДАЮ
Директор МБОУ СОШ №10
им. С.И. Холодова ст. Новощербиновская
_____ Е.М. Пидварко

ПЛАН
мероприятий по защите персональных данных
в МБОУ СОШ №10 им. С.И. Холодова ст. Новощербиновская

| № п/п | Наименование мероприятия | Срок выполнения | Примечание |
|-------|--|--|---|
| 1. | Документальное регламентирование работы с ПД | При необходимости | Разработка положения по обработке и защите персональных данных, регламента специалиста ответственного за безопасность персональных данных, либо внесение изменений в существующие |
| 2. | Получение письменного согласия субъектов ПД (физических лиц) на обработку ПД в случаях, когда этого требует законодательство | Постоянно | Письменное согласие получается при передаче ПД субъектами для обработки в ИСПДн, либо для обработки без использования средств автоматизации. |
| 3. | Пересмотр договора с субъектами ПД в части обработки ПД | При необходимости | В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона (например, в договор может быть включено согласие субъекта на обработку и передачу его ПД). Пересмотр договоров проводится при необходимости и оставляется на усмотрение организации – оператора ПД |
| 4. | Ограничение доступа работников к ПД | При необходимости (при создании ИСПДн) | В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона необходимо разграничить доступ к ПД сотрудников организации согласно (сотрудники наделяются минимальными полномочиями доступа, необходимыми для выполнения ими своих обязанностей, например, могут иметь права только на просмотр ПД). |
| 5. | Повышение квалификации сотрудников в области защиты персональных данных | Постоянно | Ответственных за выполнение работ – не менее раз в два года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за защиту персональных данных подразделения) |
| 6. | Инвентаризация информационных ресурсов | Раз в полгода | Проводится с целью выявления присутствия и обработки в них ПД |
| 7. | Выявление угроз безопасности и разработка моделей угроз и нарушителя | При необходимости | Разрабатывается при создании системы защиты ИСПДн |
| 8. | Аттестация (сертификация) СЗПД или декларирование соответствия по требованиям безопасности ПД | При необходимости | Проводится совместно с лицензиатами ФСТЭК |
| 9. | Эксплуатация ИСПД | Постоянно | |

| | | | |
|-----|--|-------------------|---|
| | и контроль безопасности ПД | | |
| 10. | Понижение требований по защите персональных данных путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер | При необходимости | В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона. |