

СОГЛАСОВАНО
Председатель п/к
от «17» июля 2019 г.

УТВЕРЖДЕНО
Директор МКОУ
«Аптряковская НОШ»
Приказ № 23
«17» июля 2019 г.

ПОЛОЖЕНИЕ
об обработке персональных данных
в муниципальном казенном общеобразовательном учреждении
«Аптряковская начальная общеобразовательная школа»

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее – Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого использования персональных данных, обрабатываемых в муниципальном казенном общеобразовательном учреждении «Аптрыковская начальная общеобразовательная школа» (далее – Оператор) в соответствии с законодательством Российской Федерации.

1.2. Настоящее Положение разработано в соответствии с:

1. Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
2. Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. Для целей настоящего Положения используются следующие основные понятия:

1. персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);
2. 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;
3. распространение персональных данных – действия, направленные на передачу персональных данных определённому 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;
4. использование персональных данных – действия с персональными данными, совершаемые работниками Оператора 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;
5. автоматизированная обработка – обработка данных, выполняемая средствами вычислительной техники;
6. блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
7. 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;
8. обезличивание персональных данных – действия, в результате которых становится невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
9. информационная система персональных данных (ИСПДн) – система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

10. защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер обеспечения конфиденциальности информации о конкретном субъекте персональных данных.

1.4. ПДн, обрабатываемые Оператором, относятся к конфиденциальной информации, порядок работы с которой регламентирован Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» и осуществляется с соблюдением строго определенных правил и условий.

2. Получение, обработка и защита персональных данных

2.1. Порядок получения ПДн

2.1.1. Все ПДн следует получать лично у субъекта ПДн. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение №1 к Положению). Оператор должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн и последствиях отказа субъекта ПДн дать письменное согласие на их получение. В случае, когда Оператор является третьей стороной, которой ПДн передаются от другого юридического лица, осуществляющего обработку ПДн, в форме согласия последнего оговаривается передача ПДн третьим лицам.

Исключением считаются случаи, в которых согласно законодательству Российской Федерации согласие не предусмотрено.

2.1.2. Оператор обрабатывает ПДн на основании следующих документов:

1. ПДн сотрудников – в целях исполнения возложенных на Оператора действующим законодательством обязанностей работодателя на основании п. 5, ч. 1, ст. 6 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», трудовых и гражданско-правовых договоров с сотрудниками, а также (при обработке ПДн в целях, отличных от исполнения обязанностей работодателя) – на основании письменного согласия субъекта ПДн;
2. ПДн обучающихся и организаторов тестирования – в целях обеспечения проведения государственной итоговой аттестации обучающихся на основании п. 2, ч. 1, ст. 6 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», ст. 98 Федерального закона 29 декабря 2012 г. «Об образовании в Российской Федерации»;
3. ПДн детей дошкольного возраста и их родителей (опекунов, представителей) – в целях обеспечения предоставления муниципальной услуги по приёму заявлений граждан, постановке на учёт и зачислению детей в общеобразовательные учреждения, реализующие основную образовательную программу дошкольного образования на основании Постановления Правительства РФ от 17.12.2009 г. №1993-р «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде», Распоряжения Правительства РФ от 25.10.2014 г. №2125-р «О создании единой системы учёта обучающихся в образовательных организациях различного типа»;
4. ПДн иных субъектов – в целях, зафиксированных в согласии на обработку ПДн на основании письменного согласия субъекта ПДн, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных».

2.1.3. Письменное согласие субъекта ПДн на обработку его ПДн должно включать в себя:

1. фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2. фамилию, имя, отчество, адрес представителя субъекта ПДн, 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 ПДн);
3. наименование и адрес Оператора;
4. цель обработки ПДн;
5. перечень ПДн, на обработку которых даётся согласие субъекта ПДн;
6. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка будет поручена такому лицу;
7. перечень действий с ПДн, на совершение которых даётся согласие, общее описание используемых Оператором способов обработки ПДн;
8. срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
9. подпись субъекта ПДн.

2.1.4. Оператор не имеет права получать и обрабатывать ПДн субъекта ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности.

2.1.5. Работники Оператора имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей.

2.1.6. Работники Оператора, получающие ПДн субъекта ПДн, обязаны соблюдать установленный в отношении этих ПДн режим конфиденциальности.

2.2. Порядок обработки ПДн

2.2.1. Обработка ПДн может осуществляться только для достижения заявленных целей их обработки.

2.2.2. При определении объёма и содержания, обрабатываемых ПДн, Оператор должен руководствоваться Конституцией РФ, Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» и иными федеральными законами в области защиты ПДн, принципом соответствия объёма и содержания обрабатываемых ПДн заявленным целям их обработки.

2.2.3. Оператор не имеет права объединять в одной базе данных ПДн, цели обработки которых не совместимы. В частности, Оператор не имеет права объединять в одной базе данных ПДн сотрудников и обучающихся.

2.2.4. При принятии решений, затрагивающих интересы субъекта ПДн, Оператор не имеет права основываться на результатах исключительно автоматизированной обработки его ПДн, кроме случаев, наличия согласия в письменной форме субъекта ПДн на принятие таких решений и случаев, предусмотренных федеральными законами.

2.2.5. Съёмные электронные носители, на которые копируются ПДн, должны быть промаркированы и учтены в Журнале регистрации, учёта и выдачи сменных носителей ПДн.

2.3. Порядок защиты ПДн

2.3.1. Защита ПДн субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Оператором за счёт его средств в порядке, установленном федеральными законами Российской Федерации в области защиты ПДн.

2.3.2. Оператор самостоятельно или с привлечением имеющих соответствующие лицензии организаций:

1. назначает лицо, ответственное за организацию обработки ПДн;
2. назначает постоянно действующую комиссию по проведению мероприятий по защите ПДн;
3. определяет и поддерживает в актуальном состоянии перечень обрабатываемых ПДн и технических средств, применяемых при их обработке;
4. составляет и поддерживает в актуальном состоянии модель угроз безопасности обрабатываемых ПДн;
5. выделяет ИСПДн и определяет требования к уровням защищенности обрабатываемых в них ПДн в соответствии с действующим законодательством;
6. назначает ответственных администраторов ИСПДн и администраторов информационной безопасности ИСПДн;
7. устанавливает правила доступа к ИСПДн и обрабатываемым ими ПДн;
8. разрабатывает и реализует систему организационных и технических мер по обеспечению безопасности ПДн, обрабатываемых в ИСПДн;
9. осуществляет учёт машинных носителей ПДн;
10. обеспечивает регистрацию действий с ПДн, обрабатываемыми в ИСПДн;
11. предпринимает меры по своевременному выявлению и предотвращению попыток несанкционированного доступа к находящимся в его распоряжении ПДн;
12. осуществляет контроль эффективности принимаемых им мер по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

2.3.3. Оператор обязан при обработке ПДн субъектов ПДн принимать необходимые организационные и технические меры для защиты ПДн от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

2.3.4. Соблюдать порядок получения, учёта и хранения ПДн субъектов ПДн.

2.3.5. Применять технические средства охраны и сигнализации.

2.3.6. Взять со всех работников, связанных с получением, обработкой и защитой ПДн субъектов ПДн, Обязательство о неразглашении ПДн (Приложение № 2 к Положению).

2.3.7. Привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту ПДн субъекта ПДн.

2.3.8. Запретить допуск к ПДн субъектов ПДн работников Оператора, не включённых в Перечень лиц, допущенных к обработке ПДн, обрабатываемых Оператором.

2.3.9. Защита доступа к электронной базе данных, содержащей ПДн субъектов ПДн, должна обеспечиваться путём использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к ПДн субъектов ПДн.

2.3.10. Оператор обязуется вырабатывать и внедрять меры защиты ПДн субъектов ПДн.

3. Хранение персональных данных

3.1. Сведения о субъектах ПДн на бумажных носителях должны храниться Оператором в специально оборудованных шкафах и сейфах, которые запираются на ключ и

опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у Ответственного за хранилища.

3.2. Обязанности по хранению сведений о субъектах ПДн, заполнению, хранению и выдаче документов, содержащих ПДн, возлагаются на Ответственного за обработку и защиту ПДн.

3.3. Съёмные электронные носители, на которых хранятся резервные копии ПДн субъектов ПДн, должны быть промаркированы и учтены в журнале регистрации, учёта и выдачи внешних носителей для хранения резервных копий ПДн.

3.4. В процессе хранения ПДн субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой ПДн, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.5. Хранение ПДн должно осуществляться не дольше, чем это необходимо для достижения целей их обработки, либо чем это определено Федеральным законом, принятым в соответствии с ним нормативным актом, договором или иным документом, являющимся основанием для обработки и хранения ПДн.

4. Передача персональных данных

4.1. Трансграничная передача ПДн Оператором не осуществляется.

4.2. Передача находящихся в распоряжении Оператора ПДн работника в пределах Российской Федерации возможна только при выполнении одного или нескольких из следующих условий:

1. имеется письменное согласие субъекта ПДн на передачу его ПДн третьему лицу, включающее наименование или фамилию, имя, отчество и адрес третьего лица, цели, сроки и способы обработки третьим лицом ПДн;
2. третье лицо является законным представителем субъекта ПДн;
3. передаваемые ПДн являются общедоступными (доступ неограниченному кругу лиц к ПДн предоставлен субъектом ПДн либо по его просьбе);
4. передача ПДн третьему лицу необходима для исполнения договора, одной из сторон которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
5. передача ПДн третьему лицу производится на основании и в порядке, предусмотренном Федеральным законом;
6. имеются иные, предусмотренные законодательством, основания для передачи ПДн третьему лицу.

4.3. Передача ПДн третьему лицу, за исключением случаев, предусмотренных пп. 2, пп. 5 п. 4.2. настоящего Положения, осуществляется в рамках заключенного между Оператором и третьим лицом договора, который в обязательном порядке включает:

1. цели и сроки обработки третьим лицом передаваемых ПДн;
2. перечень действий с передаваемыми ПДн, которые могут осуществляться третьим лицом, а также способы их осуществления;
3. обязанность третьего лица соблюдать конфиденциальность передаваемых ПДн и обеспечивать их безопасность при обработке, в т.ч. предпринимать меры по обеспечению безопасности ПДн, предусмотренные ст. 19 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» (кроме установленных законодательством случаев, когда обеспечение конфиденциальности ПДн не требуется).

В случаях, когда ПДн передаются третьему лицу на основании согласия субъекта ПДн, цели, сроки и способы обработки ПДн, включаемые в договор с третьим лицом, должны

соответствовать целям, срокам и способам обработки ПДн, указанным в согласии субъекта ПДн.

4.4. Требования безопасности, предъявляемые к процедурам передачи ПДн третьему лицу, могут включаться в условия соответствующего договора или устанавливаться иным соглашением между Оператором и третьим лицом. В тех случаях, когда процедуры передачи ПДн и (или) предъявляемые к ним требования безопасности документально не определены, они определяются лицами, ответственными за обеспечение безопасности ПДн Оператора и третьего лица совместно.

4.5. На передачу ПДн третьему лицу, осуществляемую на основании и в порядке, предусмотренном Федеральным законом, в том числе на передачу ПДн по запросу третьего лица, полномочия которого на получение соответствующих ПДн установлены Федеральным законом (органов следствия, органов государственной безопасности и т.п.), требования настоящего раздела не распространяются.

5. Уничтожение персональных данных

5.1. При необходимости уничтожения ПДн Оператор должен руководствоваться следующими требованиями:

1. уничтожение ПДн осуществляется комиссией по проведению мероприятий по уничтожению ПДн. После уничтожения ПДн составляется соответствующий акт;
2. бумажные носители ПДн должны уничтожаться при помощи специального оборудования (измельчителя бумаги) или могут быть сожжены;
3. ПДн, представленные в электронном виде, должны уничтожаться с использованием специализированного программного обеспечения, гарантирующего невозможность восстановления удаленных данных или посредством неоднократной перезаписи областей памяти, либо путём уничтожения физического носителя содержащего такие данные.

6. Внутренние проверки состояния защищенности информационной системы персональных данных

6.1. Проверка состояния защищенности ПДн, обрабатываемых Оператором осуществляется комиссией по проведению мероприятий по защите ПДн.

6.2. Комиссией составляется План мероприятий по внутреннему контролю, который утверждается директором. Назначаются исполнители Плана.

6.3. Проверка состояния защищенности осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых Оператором, требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты ПДн.

6.4. Составляется План проведения проверок защищённости ПДн, обрабатываемых Оператором, включающий в себя:

1. дату и место проведения проверки;
2. цель проверки;
3. краткие сведения об объектах и способах проверки.

6.5. Внутренняя проверка Комиссии по проведению мероприятий по защите ПДн завершается подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки защищенности ПДн, обрабатываемых Оператором.

6.6. Акт должен содержать:

1. дата, время и место составления акта;
2. дата и место проведения проверки;
3. сведения о результатах проверки, в том числе о выявленных нарушениях и их характере;
4. достоверное и обоснованное изложение состояния защищённости информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

7. Обязанности субъекта персональных данных и Оператора

7.1. В целях обеспечения достоверности ПДн субъект ПДн обязан:

1. предоставлять Оператору полные и достоверные данные о себе;
2. в случае изменения своих ПДн сообщать данную информацию Оператору.

7.2. Оператор обязан:

1. осуществлять защиту ПДн субъекта ПДн;
2. вести Журнал учёта запросов субъектов ПДн по вопросам обработки их ПДн;
3. обеспечивать хранение документации, содержащей ПДн субъектов ПДн, при этом ПДн не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

8. Права субъекта ПДн в целях защиты персональных данных

8.1. Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. В случае достижения целей обработки, правомерности запроса субъекта ПДн на уничтожение его ПДн и отсутствии требований законодательства, в соответствии с которыми обработка ПДн может быть продолжена или в случае, когда не удастся устранить нарушения в обработке ПДн, Оператор уничтожает ПДн с составлением Формы уведомления об уничтожении.

8.2. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн на основе Формы запроса субъекта ПДн на доступ к своим ПДн, в том числе содержащей:

1. подтверждение факта обработки ПДн Оператором;
2. правовые основания и цели обработки ПДн;
3. цели и применяемые Оператором способы обработки ПДн;
4. наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
5. обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения;
6. сроки обработки ПДн, в том числе сроки их хранения;
7. порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
8. информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;

9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
10. иные сведения, предусмотренные Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» или другими федеральными законами.

8.3. Субъект ПДн имеет право на определение представителей для защиты своих законных интересов.

8.4. Субъект ПДн имеет право требовать исключить или исправить неверные или неполные ПДн, а также ПДн, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных». В случае исправления допущенных нарушений Оператором заполняется Форма уведомления об устранении нарушений, допущенных при обработке ПДн (Приложение №7), в копию отсылки Уведомления включается субъект ПДн.

8.5. Субъект ПДн имеет право требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта ПДн, обо всех произведённых в них исключениях, исправлениях или дополнениях.

8.6. Субъект ПДн имеет право на обжалование в судебном порядке любых неправомерных действий или бездействия Оператора при обработке и защите его ПДн.

8.7. Процедуры рассмотрения запросов субъектов ПДн или их представителей регламентируется Правилами рассмотрения запросов субъектов ПДн или их представителей (Приложение №8)

9. Особенности обработки ПДн без использования средств автоматизации

9.1. Типовые бумажные формы, предполагающие включение в них ПДн:

1. заявление о приёме на работу;
2. личная карточка работника (форма Т-2);
3. обязательство о неразглашении информации ограниченного доступа;
4. согласие на обработку персональных данных;
5. личный листок по учёту кадров.

9.2. Лица, осуществляющие обработку ПДн без использования средств автоматизации (в том числе сотрудники организации или лица, осуществляющие такую обработку по договору) должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации.

9.3. Ведение журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимых для однократного пропуска субъекта ПДн в помещения организации или в иных аналогичных целях не предполагается.

9.4. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

9.5. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

10. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

10.1. Лица, виновные в нарушении требований федеральных законов Российской Федерации, несут предусмотренную законодательством Российской Федерации ответственность.

10.2. Моральный вред, причинённый субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, установленных федеральными законами, а также нарушения требований к защите ПДн подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесённых субъектом ПДн убытков.

