

РАССМОТРЕНО

на заседании педагогического Совета
от "17" 05 2017 г.
протокол № 6



ПОЛОЖЕНИЕ

**о порядке обработки и обеспечении безопасности
персональных данных осуществляемой в ГБОУ РК
«АЛУПКИНСКАЯ САНАТОРНАЯ ШКОЛА-
ИНТЕРНАТ»**

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных в ГБОУ РК «Алупкинская санаторная школа-интернат».

1.2. Сведения о персональных данных субъектов относятся к числу конфиденциальных (составляющих охраняемую законом тайну).

1.3. Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;
- в случае их общедоступности;
- в других случаях, предусмотренных федеральными законами.

Перечень помещений, предназначенных для обработки персональных данных субъектов ГБОУ РК «Алупкинская санаторная школа-интернат», утверждается директором;

1.4. В целях настоящего Положения используются следующие термины и понятия:

- **персональные данные (далее - ПДн)** - 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;

- **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;

- **информационная система персональных данных** - информационная 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;

- **обработка персональных данных без использования средств автоматизации (неавтоматизированная)** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлечённых из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

- **конфиденциальность персональных данных** – обязательное, для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, воспитанников и родителей (законных представителей) воспитанников ГБОУ РК «Алупкинская санаторная школа-интернат», требование не допускать их распространения без согласия работников и родителей (законных представителей) воспитанников ГБОУ РК «Алупкинская санаторная школа-интернат» или иного законного основания;
- **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных граждан или в результате которых уничтожаются материальные носители персональных данных граждан;
- **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному гражданину;
- **информационная система персональных данных (далее – ИСПДн)** - Информационные системы персональных данных; совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Субъекты персональных данных

2.1. К субъектам ПДн, ПДн которых обрабатываются в ГБОУ РК «Алупкинская санаторная школа-интернат», относятся:

- 1) Работники ГБОУ РК «Алупкинская санаторная школа-интернат»;
- 2) Обучающиеся и их законные представители.

3. Состав ПДн

3.1. Состав ПДн, обрабатываемых ГБОУ РК «Алупкинская санаторная школа-интернат», определён в «Перечне ПДн, обрабатываемых в ГБОУ РК «Алупкинская санаторная школа-интернат».

3.2. При поступлении на работу работник, предоставляет ПДн о себе в документированной форме, в соответствии с требованиями Трудового кодекса РФ и иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ;

3.3. При приёме обучающихся в ГБОУ РК «Алупкинская санаторная школа-интернат», их родители (законные представители) предоставляют документы, перечень которых, установлен приказом по ГБОУ РК «Алупкинская санаторная школа-интернат»;

4. Основные условия проведения обработки персональных данных

4.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта ПДн, составленного по форме согласно (Приложению № 1, 2 к настоящему Положению), за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

- после принятия необходимых мер по защите персональных данных при их обработке с использованием средств автоматизации и без использования таковых.

4.2. В ГБОУ РК «Алупкинская санаторная школа-интернат» приказом директора назначается сотрудник, ответственный за защиту персональных данных, сотрудник ответственный за организацию обработки ПДн, ответственные лица за обработку ПДн и определяется перечень лиц, допущенных к обработке ПДн.

4.3. Лица, допущенные к обработке ПДн, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей ПДн (Приложение 3 к настоящему Положению).

4.4. Запрещается:

- обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод ПДн под диктовку.

4.5. Информация о ПДн может содержать:

- на бумажных носителях;
- в ИСПДн, перечень и состав которых определяется комиссией по классификации ИСПДн в ГБОУ РК «Алупкинская санаторная школа-интернат»;

4.6. ГБОУ РК «Алупкинская санаторная школа-интернат» определяет категории обрабатываемых ПДн, их объем и цели обработки, руководствуясь Конституцией РФ, 152-ФЗ «О персональных данных»;

4.7. Обработка ПДн осуществляется на основании «Согласия на обработку ПДн».

5. Порядок определения защищаемой информации

5.1. В ГБОУ РК «Алупкинская санаторная школа-интернат» на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента Российской Федерации 6 марта 1997 года № 188, определяется и утверждается перечень ПДн, не относящихся к государственной тайне и перечень информационных систем персональных данных (далее - ИСПДн) подлежащих защите.

5.2. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки ПДн, утверждается перечень обрабатываемых ПДн.

6. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

6.1. Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями с постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

6.2. Оператором персональных данных осуществляется классификация информационных систем персональных данных в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в зависимости от категории обрабатываемых данных и их количества.

6.3. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6.4. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных;

7. Порядок обработки персональных данных без использования средств автоматизации

7.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

7.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

7.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- хранение персональных данных должно соответствовать требованиям законодательства в части обработки персональных данных и быть подчинено требованиям разработанной инструкции по обращению с персональными данными при их неавтоматизированной обработке;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

7.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, при необходимости получения письменного согласия на обработку персональных данных;

- в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

7.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

7.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

7.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

7.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

7.10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

8. Ответственность должностных лиц

8.1. Ответственные лица, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

8.2. Ответственным лицам за обработку ПДн ознакомиться под роспись с положениями данного Положения в Листе ознакомления.