

Рассмотрено и принято
на заседании
Педагогического совета
протокол №1
от 27 августа 2019 года

УТВЕРЖДАЮ
Директор ЧОУ «Ор Авнер»
Н.Д. Дойч
Н.Д. Дойч
Приказ №22-од
от 30 августа 2019 г.

Частное образовательное учреждение «Общеобразовательная школа «Ор Авнер» (свет Авнера)»

Положение об обработке персональных данных работников

Глава 1. Общие положения

1.1. Положение об обработке персональных данных работников Частного образовательного учреждения «Общеобразовательная школа «Ор Авнер» (свет Авнера)» (далее – Положение) определяет порядок обработки и защиты персональных данных работников ЧОУ «Ор Авнер».

1.2. Положение обязательно для исполнения всеми должностными лицами ЧОУ «Ор Авнер», неисполнение Положения влечет материальную, дисциплинарную, гражданскую, административную и уголовную ответственность.

1.3. Целями Положения являются:

- 1) установление порядка обработки персональных данных с использованием средств автоматизации или без использования таких средств;
- 2) определение прав и обязанностей работников ЧОУ Работодателя в области обработки персональных данных;
- 3) организация и обеспечение защиты прав работников ЧОУ при обработке их персональных данных.

1.4. В Положении используются следующие основные термины:

Понятие	Значение
Документы, содержащие персональные данные работника	Копии личных документов работника (паспорт, диплом, военный билет, водительское удостоверение, заграничный паспорт, свидетельство о рождении, документы об образовании, ИНН, страховое свидетельство, медицинские документы, и т.п.), анкета (предоставляется по желанию работника), заявления, трудовая книжка, личная карточка работника по форме Т-2, экземпляр трудового договора и изменений (дополнительных соглашений) к нему, приказы по личному составу, книга учета движения кадров и т.д.
Персональные данные работника	Любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, дата и место рождения, семейное, социальное и имущественное положение, образование, профессия, доходы и другая информация, необходимая работодателю в связи с

	трудовыми отношениями и касающаяся конкретного работника.
Информационная система персональных данных	Информационная система, представляющая собой упорядоченную 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 них.
Конфиденциальность персональных данных	Обязательное для соблюдения оператором или иным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.
Обработка персональных данных работников	Действия (операции) с персональными данными работника, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе и передачу), обезличивание, блокирование и уничтожение персональных данных работника.

1.5. К персональным данным работников ЧОУ относятся следующие категории персональных данных:

- непосредственно персональные данные (фамилия, имя, отчество, дата и место рождения, семейное, социальное и имущественное положение, образование, профессия, доходы);
- специальные категории персональных данных (национальная принадлежность; состояние здоровья);
- биометрические категории персональных данных (фото).

Глава 2. Порядок обработки персональных данных, осуществляемой без использования средств автоматизации

2.1. Доступ к персональным данным работников ЧОУ имеют:

- 1) директор, заместители директора (доступ к персональным данным работников в связи с необходимостью исполнения ими своих должностных обязанностей);
- 2) специалист по кадрам (доступ к персональным данным работников в связи с необходимостью исполнения ими своих должностных обязанностей);
- 3) работник (доступ к своим персональным данным);
- 4) органы государственной власти, контрольные и надзорные органы (в рамках своих полномочий в соответствии с федеральными законами).

2.2. Должностные лица, имеющие доступ к персональным данным работников ЧОУ, при обработке персональных данных должны соблюдать следующие требования:

1) все персональные данные работника ЧОУ следует получать у него лично. Если по уважительным причинам это невозможно, то привлекается третья сторона, с письменного согласия самого работника. Работодатель сообщает работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

2) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни;

3) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в политических партиях, общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;

4) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.3. Порядок хранения и использования персональных данных работников устанавливается с соблюдением требований Трудового кодекса Российской Федерации и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

1) документы, содержащие персональные данные работника, хранятся в сейфе или специально оборудованном несгораемом шкафу, запирающемся на ключ, доступ к которому имеют директор и специалист по кадрам;

2) документы по учету кадров и документы, содержащие сведения о работниках и их трудовой деятельности, хранятся в личных делах работников, которые формируются и поддерживаются в актуальном состоянии специалистом по кадрам в течение всего срока работы работника;

3) после увольнения работника его личное дело подлежит хранению у Работодателя в установленном порядке в течении 75 лет или до момента ликвидации ЧОУ. При ликвидации ЧОУ личное дело работника передается на хранение в государственный архив в установленном порядке;

4) персональные данные работников могут храниться в электронном виде в информационной системе персональных данных (электронной базе данных); доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается системой;

5) ответственность за хранение (сохранность) документов, связанных с трудовой деятельностью работников, несет персонально специалист по кадрам;

6) специалист по кадрам может снимать копии с документов, делать выписки, составлять аналитические и иные справки, изымать (заменять) документы, хранящиеся в личных делах работников, исключительно в рамках своих должностных обязанностей;

7) выдача копий документов, содержащих персональные данные работников, осуществляется в соответствии со ст. 62 Трудового кодекса Российской Федерации

Федерации уполномоченными лицами, имеющими доступ к персональным данным работников;

8) специалист по кадрам выдает работнику по его письменному заявлению (по форме согласно Приложению 1 Положения) безвозмездно копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводе на другую работу, приказа об увольнении и др.), а также выписки из трудовой книжки и справки, содержащие данные работника о его трудовой деятельности ЧОУ;

9) копии документов, связанных с работой, заверяются надлежащим образом: на копии проставляются заверительная надпись «Верно», наименование должности лица, заверившегося копию, личная подпись, расшифровка подписи (инициалы, фамилии), дата заверения, оттиск печати.

2.4. Право заверять копии трудовых книжек и других документов работников ЧОУ, делать выписки из них имеет директор.

2.5 В случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», обработка персональных данных осуществляется только с согласия работника в письменной форме (по форме согласно Приложениям 2 к Положению).

2.6. Ответ на запрос органов государственной власти, контрольных и надзорных органов о предоставлении персональных данных работника оформляется специалистом по кадрам письмом ЧОУ, которое подписывается директором ЧОУ (при необходимости с приложением копий запрошенных документов). Содержание данного письма (включая любые приложения к нему) является конфиденциальным.

Глава 3. Права и обязанности Работодателя

3.1. Работодатель обязан:

1) не сообщать персональных данных работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, установленных федеральными законами;

2) не сообщать персональных данных работника в коммерческих целях без его письменного согласия;

3) предупредить лиц, получающих персональные данные работника о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность;

4) осуществлять передачу персональных данных работника в соответствии с Положением, с которым работник должен быть ознакомлен под личную подпись;

5) разрешить доступ к персональным данным работников только специально уполномоченными лицами, при этом указанные лица имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных должностных обязанностей;

6) не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником должностных обязанностей;

7) передавать персональные данные работника представителем работника в порядке, установленном Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их должностных обязанностей.

3.2. Работодатель имеет право запрашивать у работника достоверные персональные данные, необходимые Работодателю в связи с трудовыми отношениями, при приеме на работу и в случаях изменения (дополнения) персональных данных.

Глава 4. Права и обязанности работников

4.1. Работник обязан:

1) предоставлять Работодателю достоверные персональные данные;

2) свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами;

3) определение своих представителей для защиты своих персональных данных;

4) доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по его выбору;

5) требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Положения. При отказе Работодателя исключить или исправить персональные данные работник имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

6) требование об извещении Работодателем всех лиц, которыми ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

7) обжалование в суд любых неправомерных действий или бездействия Работодателя при обработке и защите персональных данных работника.

Глава 5. Общедоступные источники персональных данных работников

5.1. В целях информационного обеспечения Работодателем могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, дата рождения, адрес, номер телефона, сведения о профессии и иные персональные данные предоставленные работником.

5.2. Сведения о работнике могут быть в любое время исключены из общедоступных источников персональных данных по требованию самого

работника либо по решению суда или иных уполномоченных государственных органов.

Глава 6. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

6.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

6.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.3. при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, 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;

2) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку персональных данных;

3) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

4) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

6.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

1) 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;

2) 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.

6.5. 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).

6.6. Правила, предусмотренные пунктами 6.4. и 6.5. настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработки зафиксированных на отдельном материальном носителе персональных данных и информации, не являющейся персональными данными.

6.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.8. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом Работодателя.

Глава 7. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

7.1. Информационные системы персональных данных представляют собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее – информационные системы)

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники,

информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

7.2. Исключается несанкционированный, в том числе случайный, доступ к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространения персональных данных, а также иных несанкционированные действия.

7.3. Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

7.4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

7.5. При обработке персональных данных в информационной системе обеспечиваются:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

7.6. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с

использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документации;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использование средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятия мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

7.7. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного руководителем.

7.8. запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 14 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора.

7.9. При обнаружении нарушений порядка предоставления персональных данных оператор незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Глава 8. Ответственность

8.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных работника, несут уголовную, административную, гражданскую, материальную и дисциплинарную ответственность, вплоть до увольнения по соответствующим основаниям, в порядке, установленном законодательством Российской Федерации.

Директору ЧОУ «Ор Авнер»

от _____

ЗАЯВЛЕНИЕ

Прошу выдать мне:

- заверенную (ые) копию (ии) документа (ов), связанного (ых) с моей работой:

(наименование документа и его краткое содержание)

В _____ (цифрами) (_____ (прописью)) экземпляре (ах).

- Справку с места работы:

(перечислить сведения, которые необходимо указать в справке)

В _____ (цифрами) (_____ (прописью)) экземпляре (ах).

(наименование должности)

(личная подпись)

Копия (ии) документа (ов) / справка (и) получена (ы):

« _____ » _____ 20__ г.

(дата)

(личная подпись)

Директору ЧОУ «Ор Авнер»
Дойч Н.Д.

(ФИО Работника)

(должность)

Паспортные данные _____

Домашний адрес: _____

Заявление

Я, _____, даю свое согласие на сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передачу строго определенному кругу лиц), обезличивание, блокировку и уничтожение своих персональных данных:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- семейное, социальное положение;
- образование;
- профессия;
- доходы, полученные мной в данном учреждении, - для передачи в налоговую инспекцию по форме 2-НДФЛ и органы ПФР индивидуальных сведений о начисленных страховых взносах на обязательное пенсионное страхование и данных о трудовом стаже;
- контактный рабочий телефон;
- контактный мобильный телефон;
- сведения о состоянии на воинском учете (не надо, если женщина не состоит);
- ФИО моих детей и место их учебы (для получения социального налогового вычета);
- паспортные данные;
- ИНН;
- страховой номер индивидуального лицевого счета;
- номер банковской карты;
- справка об отсутствии противопоказаний к данному виду деятельности;
- данные флюорографического обследования;
- данные по вакцинации;
- данные результатов профилактических медицинских осмотров;
- фотография.

Передача персональных данных разрешается на срок действия трудового договора. Настоящее заявление может быть отозвано в случае нарушения работодателем законодательства в области защиты персональных данных либо по моему заявлению. Права и обязанности в области защиты персональных данных мне разъяснены.

Дата

Подпись

Расшифровка подписи _____