

«УТВЕРЖДАЮ»

Директор ГКУ СО

«Тольяттинский социально – реабилитационный центр «Гармония»

П. А. Зипнагулина

2012 г.



ПОЛОЖЕНИЕ о порядке обработки персональных данных работников и воспитанников в Государственном казенном учреждении Самарской области «Тольяттинский социально – реабилитационный центр «Гармония»

1. Общие положения

1.1. Настоящее Положение о порядке обработки персональных данных в Государственном казенном учреждении Самарской области «Тольяттинский социально-реабилитационный центр для несовершеннолетних «Гармония» (далее – Положение) имеет своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Положение определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников и 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, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативно правовыми актами, операторами, являющимися государственными или муниципальными органами», правовых актов уполномоченных федеральных органов исполнительной власти.

1.4. Все работники Государственного казенного учреждения Самарской области «Тольяттинский социально-реабилитационный центр для несовершеннолетних «Гармония» (далее – Учреждение) должны быть ознакомлены с настоящим Положением под роспись.

1.5. Положение вступает в силу с момента его утверждения директором и действует до введения нового Положения.

2. Основные понятия и состав персональных данных

2.1. В целях настоящего Положения используются следующие термины и понятия:
персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
оператор - государственный орган, муниципальный орган, юридическое или физическое 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;

работник – физическое лицо, состоящее в трудовых отношениях с оператором;

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;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных 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.

2.2. К персональным данным работника относятся:

- сведения, содержащиеся в основном документе, удостоверяющем личность субъекта;

- информация, содержащаяся в трудовой книжке работника;

- сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу;

- сведения об образовании, квалификации или наличии специальных знаний или подготовки;

- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;

- сведения о семейном положении работника;

- информация медицинского характера, в случаях, предусмотренных законодательством

- сведения о заработной плате работника;

- сведения о социальных льготах;

- место работы или учебы членов семьи;

- содержание трудового договора;

- подлинники и копии приказов по личному составу;
- основания к приказам по личному составу;
- документы, содержащие информацию по повышению квалификации и переподготовке сотрудника, его аттестация, служебное расследование
- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником.

2.3. К персональным данным воспитанников, получаемым и подлежащим хранению в Учреждении в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах, медицинских картах:

- документы, удостоверяющие личность воспитанника (свидетельство о рождении или паспорт);
- полис обязательного медицинского страхования;
- паспортные данные родителей (законных представителей) воспитанника;
- документы о состоянии здоровья (амбулаторная карта из поликлиники, история развития ребенка);
- сведения о месте проживания (акт обследования жилищно-бытовых условий проживания несовершеннолетнего);
- сведения о составе семьи;
- документы, содержащие сведения о состоянии несовершеннолетнего по результатам МППК (медико-психолого-педагогическая комиссия) и ПМПК (психолого-медико-педагогическая комиссия);
- иные сведения, содержащие персональные данные и необходимые оператору для качественного выполнения своих функциональных обязанностей (коррекционно-реабилитационной работы с несовершеннолетними, в возрасте от 3 до 18 лет).

3. Обработка персональных данных.

3.1. Получение персональных данных

3.1.1. Обработка персональных данных работников осуществляется исключительно в целях обеспечения законов и иных нормативно-правовых актов, содействия работникам в обучении и продвижении по службе, а также обеспечения личной безопасности работников, сохранности имущества, контроля количества и качества выполняемой работы.

Обработка персональных данных воспитанников (несовершеннолетних, оказавшихся в трудной жизненной ситуации) осуществляется исключительно в целях оказания социально-бытовой, социально-медицинской, социально-педагогической, социально-психологической, социально-правовой, социально-экономической и иной социальной помощи (услуг).

3.1.2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку оператором свободно, своей волей и в своем интересе. Согласие на обработку должно быть конкретным, информированным и сознательным. *Форма согласия на обработку персональных данных представлена в приложении № 1 к настоящему положению.*

Согласие на обработку персональных данных воспитанников (несовершеннолетних, находящихся в трудной жизненной ситуации) Учреждения следует получать от его законных представителей (родителей, опекунов, попечителей).

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в п. 2-11 ч. 1 ст. 6, ч.2 ст.10 и ч.2 ст.11 Федеральном законе «О

персональных данных». *Форма отзыва согласия представлена в приложении № 2 к настоящему положению.*

3.2. Хранение персональных данных

3.2.1. Хранение персональных данных работников осуществляется специалистом по кадрам и бухгалтерией, на бумажных и электронных носителях с ограниченным доступом.

3.2.2. Подразделения, хранящие персональные данные воспитанников на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно п.6 настоящего Положения.

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

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

- 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.

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

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

3.3. Передача персональных данных

3.3.1. 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. *Форма согласия субъекта на передачу представлена в приложении № 3 к настоящему положению;*
- 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;

3.3.2. При устройстве на работу (или поступлении несовершеннолетнего) в Учреждение, специалист по кадрам (или социальный педагог) дает разъяснения субъекту персональных данных юридические последствия отказа предоставить свои персональные данные. *Типовая форма разъяснений представлена в приложении № 4 к настоящему положению.*

3.3.3. Внутренний доступ (доступ внутри организации) к персональным данным субъекта (в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных, и только в части, касающейся соответствующего направления деятельности) имеют сотрудники учреждения согласно списку. *Список должностей работников Учреждения, допущенных к обработке персональных данных (либо имеющих к ним доступ) в связи с выполнением своих служебных (трудовых) обязанностей представлен в приложении № 5 к настоящему положению.*

3.3.4. Лица, допущенные к обработке персональных данных, как с помощью информационных систем персональных данных, так и без использования средств автоматизации, в обязательном порядке подписывают уведомление о порядке обработки персональных данных (воспитанников и работников) и обязательство о неразглашении информации, содержащей персональные данные. *Форма уведомления и обязательства представлена в приложении № 6, 7 к настоящему положению.*

3.3.5. Внешний доступ

К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

инспекции труда

Прокуратура

налоговые инспекции

правоохранительные органы

военкоматы

страховые агентства

пенсионные фонды

подразделения федеральных и муниципальных органов управления

3.3.6. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством Российской Федерации.

3.3.7. Другие организации:

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариального заверенного заявления работника.

3.3.8. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ).

3.4. **Права и обязанности субъектов персональных данных и оператора** изложены в *правилах рассмотрения запросов субъектов персональных данных и их представителей, содержащихся в приложении № 8 к настоящему положению.*

4. Правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке.

4.1. К правовым мерам защиты относятся действующие законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе

ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

4.2. Организационные меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

4.2.1. Приказом директора назначается сотрудник, ответственный за организацию обработки персональных данных, а также сотрудники ответственные за сбор, хранение и обработку персональных данных работников и воспитанников.

4.2.2. Лицо, ответственное за организацию обработки персональных данных, обязано:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

4.2.3. Организационные меры в Учреждении заключаются:

4.2.3.1. В разработке и последующем ознакомлении сотрудников со следующими документами:

- список помещений Учреждения, в которых обрабатываются персональные данные и доступ к ним;
- инструкции (по работе пользователей в ИСПДн, администратора безопасности информации, пользователя при возникновении внештатных ситуаций, ответственного за организацию обработки персональных данных, по проведению антивирусного контроля);
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении;
- разработка и принятие иных документов, направленных на обеспечение информационной безопасности Учреждения.

4.2.3.2. В разработке и принятии следующих мер:

- определение лиц, допущенных к обработке персональных данных (либо имеющих к ним доступ) в связи с выполнением своих служебных (трудовых) обязанностей;
- установление и утверждение перечня персональных данных, информационных систем, места хранения персональных данных (материальных носителей);
- установление и утверждение условий обработки и категорий персональных данных, обработка которых в Учреждении, осуществляется как с использованием, так и без использования средств автоматизации;
- разработка и принятие иных мер, направленных на обеспечение информационной безопасности Учреждения.

4.3. Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты

4.3.1. Технические меры по защите персональных данных включают в себя:

исключение возможности несанкционированного доступа к персональным данным в ГКУ СО «Тольяттинский СРЦН «Гармония» лицам, не допущенным к обработке персональных данных в установленном порядке;

установку, настройку и сопровождение технических и программных средств защиты информации (в том числе шифровальных (криптографических) средств, средств предотвращения несанкционированного доступа и утечки информации по техническим каналам.

5. Условия обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

5.1. С использованием средств автоматизации (АРМ «Отдел кадров» и АРМ «1С Бухгалтерия 7.7») оператор обрабатывает *персональные данные работников. Перечень, сроки хранения и тип носителя сведений содержатся в приложении № 9 к настоящему положению.*

5.2. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативных правовых актов уполномоченных федеральных органов исполнительной власти.

5.3. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

при отсутствии установленных и настроенных сертифицированных средств защиты информации;

при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

6. Условия обработки персональных данных без использования средств автоматизации

6.1. Без использования средств автоматизации (ИСПДн «Медицина», «Социально-правовая помощь», «Психодиагностика») оператор обрабатывает *персональные данные воспитанников. Перечень, сроки хранения и тип носителя сведений содержатся в приложении № 10 к настоящему Положению.*

6.2. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

6.4. При неавтоматизированной обработке персональных данных на материальных носителях:

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

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

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

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

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

6.6. 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.

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

К каждому электронному носителю оформляется описание файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

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

6.9. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки путем подписания уведомления.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ).

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

7.1. 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.