Государственное казенное учреждение социального обслуживания Свердловской области «Социально-реабилитационный центр для несовершеннолетних «Синарский» города Каменска-Уральского»

УТВЕРЖДАЮ:
Директор государственного казенного учреждения социального обслуживания Свердловской области «Социально-реабилитационный центр для несовершеннолетних «Синарский» города Каменска-Уральского»
_____
Ю.Ю. Лесунова
«*30*» *ноября* 2021 г.

Принято на общем собрании работников учреждения
Протокол № *3*
«*30*» ноября 2021 г.

Приказ по учреждению № *180-од-1*
«*30*» *ноября* 2021 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников и воспитанников государственного казенного учреждения социального обслуживания Свердловской области «Социально-реабилитационный центр для несовершеннолетних «Синарский» города Каменска-Уральского»

I. Общие положения

1.1. Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников и воспитанников учреждения. Под сотрудниками подразумеваются лица, имеющие трудовые отношения с государственным казенным учреждением социального обслуживания Свердловской области «Социально-реабилитационный центр для несовершеннолетних «Синарский» города Каменска-Уральского» (далее – учреждение).

1.2. Целью Положения является развитие комплексных мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

1.3. Основанием для разработки данного Положения являются:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях;
- Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ;

Федеральный закон Российской Федерации «О персональных данных» от 27.07.2006 г. № 152-ФЗ;

- другие нормативно-правовые акты.

1.4. Положение и изменения к нему вводятся приказом по основной деятельности учреждения и утверждаются директором. Все сотрудники учреждения должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

II. Понятие и состав персональных данных

2.1. Под персональными данными сотрудников и воспитанников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника и воспитанника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

- все биографические сведения сотрудника и воспитанника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора (эффективного контракта);
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки и трудовые книжки сотрудников или сведении о трудовой деятельности работников;
- основания приказов по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным сотрудника и воспитанника.

Указанные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

2.2. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.3. Собственником информационных ресурсов (персональных данных) является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

2.4. Держателем персональных данных является работодатель (оператор), которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функции владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.5. Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям своим заместителям, руководителям структурных подразделений, работа которых требует знаний персональных данных работников или связана с обработкой этих данных.

2.6. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

III. Принципы обработки персональных данных

3.1. Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

3.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника и воспитанника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников и воспитанников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

3.4. Не допускается получение и обработка персональных данных сотрудника и воспитанника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

3.5. При принятии решений относительно сотрудника и воспитанника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.6. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

3.7. Пакет анкетно-биографических и характеризующих материалов (далее - пакет) сотрудника и воспитанника формируется после издания приказа о его приеме на работу или поступлении в учреждение. Пакет содержит документы, содержащие данные сотрудника, в порядке, отражающем процесс приема на работу.

3.8. Пакет пополняется на протяжении всей трудовой деятельности сотрудника или проживания воспитанника в данном учреждении.

3.9. Инспектор по кадрам, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявляемыми документами.

3.10. Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

3.11.При обработке персональных данных сотрудников и воспитанников работодатель в лице директора учреждения вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников и воспитанников на базе современных информационных технологий.

3.12. Сотрудник обязан:

– передавать работодателю или его представителю комплекс достоверных, документированных персональных даннвх, состав которых установлен Трудовым кодексом Российской Федерации.

– своевременно сообщать работодателю об изменении своих персональных данных.

3.13. Сотрудник имеет право на:

– полную информацию о своих персональных данных и обработке этих данных;

– свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации;

– определение своих представителей для защиты своих персональных данных;

– доступ к относящимся к нему медицинским данным с помощью медицинского работника по своему выбору;

– требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя

исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения.

– требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

IV. Доступ к персональным данным

4.1. Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри учреждения исключительно для обработки и использования в работе.

4.2. Внешний доступ. К числу массовых потребителей персональных данных вне учреждения можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- банки;
- органы статистики;
- страховые агентства;
- отделы военного комиссариата;
- органы социального страхования:
- пенсионные фонды;
- органы опеки и попечительства;
- Министерство социальной политики Свердловской области;
- подразделения муниципальных органов самоуправления.

4.3. Внутренний доступ. Внутри учреждения к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- директор;
- специалист по кадрам;
- сотрудники бухгалтерии;
- заместители директора;
- социальный педагог;
- медицинские работники.

4.4. После увольнения сотрудника или выпуска воспитанника из учреждения документы по личному составу передаются на хранение.

V. Передача персональных данных

5.1. При передаче персональных данных сотрудника или воспитанника директор должен соблюдать следующие требования:

Передача внешнему потребителю:

– 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;

– при передаче персональных данных сотрудника или воспитанника потребителям за пределы учреждения работодатель не должен сообщать данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника или в случаях, установленных федеральным законом;

– ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения директора учреждения и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;

– не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;

– по возможности персональные данные обезличиваются.

Передача внутреннему потребителю:

5.2. Работодатель вправе разрешать доступ к персональным данным сотрудников и воспитанников. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников и воспитанников.

VI. Защита персональных данных

6.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.3. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.

6.4. «Внутренняя защита». Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами учреждения.

Для защиты персональных данных сотрудников и воспитанников необходимо соблюдать ряд мер:

– ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

– строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

– рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

– знание сотрудниками требований нормативно-методических документов по защите информации и сохранении тайны;

– наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

– определение и регламентация состава сотрудников, имеющих право доступ (входа) в помещение, в котором находится вычислительная техника;

– организация порядка уничтожения информации;

– своевременное выявление нарушения требований разрешительной системы доступа сотрудниками;

– воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

– не допускается выдача личных дел сотрудников и воспитанников на рабочие места заместителей директора. Личные дела могут выдаваться на рабочие места только директору учреждения, и в исключительных случаях, по письменному разрешению директора учреждения;

– персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

6.5. «Внешняя защита». Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия труднопреодолимые препятствия для лиц, пытающихся

совершить несанкционированный доступ к информационным ресурсам, может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

Для защиты персональных данных сотрудников и воспитанников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим учреждения;
- порядок охраны территории, зданий, помещений, транспортных средств.

VII. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

7.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет ответственность за сохранность носителя и конфиденциальной информации.

7.3. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.