


Министерство социальной политики Свердловской области
государственное казенное учреждение социального обслуживания Свердловской области
«Социально-реабилитационный центр для несовершеннолетних
Нижнесергинского района»

Принято:
Общее собрание работников
Протокол № 2
От «09» 08 2016г.

Утверждаю:
Приказ № 111-ОД от 10.08.2016 г.
Директор государственного казенного
учреждения социального обслуживания
Свердловской области «Социально-
реабилитационный центр для
несовершеннолетних Нижнесергинского
района»

И.В.Мальцева

ПОЛОЖЕНИЕ

«О защите персональных данных»

Государственного казенного учреждения социального обслуживания
Свердловской области «Социально-реабилитационный центр для
несовершеннолетних Нижнесергинского района»

Положение

О защите персональных данных работников государственного казенного учреждения социального обслуживания Свердловской области «Социально-реабилитационный центр для несовершеннолетних Нижнесергинского района» (далее Положение)

1. Общие положения

Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса, Кодекса об административных правонарушениях РФ, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального Закона от 26.07.2006 г. № 149-ФЗ «Об информации, информатизации и защите информации», Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения – 75 лет, если иное не определено законом.

Настоящее Положение является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

Персональные данные работника – информация, необходимая директору Центра в связи с трудовыми отношениями и касающаяся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

В состав персональных данных работника входят:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

- копии отчетов, направляемые в органы статистики.

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

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина директор и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечении личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника, директор Центра должен руководствоваться Конституцией РФ, Трудовым кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников. Если персональные данные работника можно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него, должно быть получено письменное согласие. Директор должен сообщить 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.

3.2.4. Директор Центра и его представители не имеют права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных, бытовых, личных отношениях) могут быть получены и обработаны только с его письменного согласия.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ:

- Директор;
- Сотрудники бухгалтерии;
- Сотрудники кадров;
- Руководители структурных подразделений.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда сотрудникам, затруднения реализации прав и свобод граждан РФ. Ограничение прав граждан РФ на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.6. Директор Центра должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника. Исключение составляют случаи, когда это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных федеральным законодательством;

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

- предупредить лиц, получающих персональные данные работника, 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 работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.7. Передача данных потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

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

3.9. Не допускается отвечать на вопросы, связанные с передачей персональной информацией по телефону или факсу.

3.10. Хранение персональных данных должно происходить в порядке, исключающем их утрату или неправомерное использование.

3.11. При принятии решений, затрагивающих интересы работника, директор основывается не только на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения, но и учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

Право доступа к персональным данным сотрудника имеют:

- директор Центра;

- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);

- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;

- сам работник, носитель данных;

- другие сотрудники организации при выполнении ими своих служебных обязанностей.

Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора Центра.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне Центра можно отнести:

- государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды.

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.3. Организации, в которых сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.4. Другие организации. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организацией только с письменного запроса на бланке организации. С приложением копии нотариально заверенного заявления работника.

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

5. Защита персональных данных

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.

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.

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 компании.

Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена директором Центра за счет его средств в порядке, установленном федеральным законом.

«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, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами Центра.

Для обеспечения внутренней защиты персональных данных работников, необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником 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 работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника; - организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа работникам подразделения; - воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей.

Личные дела могут выдаваться на рабочие места только директору, работникам бухгалтерии и в исключительных случаях по письменному разрешению директора, руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

Защита персональных данных сотрудника на электронных носителях. Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается руководителю информационно-аналитического отделения.

«Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и трудно преодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа 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 Центра, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

По возможности персональные данные обезличиваются.

Кроме мер защиты персональных данных, установленных законодательством, директор, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивают сохранность полной и точной информации о нем.

6.2. Работники и их представители должны быть ознакомлены под расписку с документами Центра, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у директора или его представителей, работник имеет право: - требовать исключения или исправления неверных или неполных персональных данных; - на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные; - персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения; - определять своих представителей для защиты своих персональных данных; - на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

- передавать директору Центра или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

- своевременно сообщать об изменениях своих персональных данных.

6.5. Работники ставят директора Центра в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники могут отказаться дать разрешение на обработку персональных данных, поскольку это может повлечь причинение морального, материального вреда.

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

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Директор Центра, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник Центра, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

Должностные лица, в обязанности которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной

информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с Уголовным кодексом Российской Федерации.