

**Положение
о защите персональных данных
автономного учреждения социального обслуживания населения Тюменской области и
дополнительного профессионального образования
«Региональный социально-реабилитационный центр для несовершеннолетних «Семья»
и
Филиала АУ СОН ТО и ДПО «РСРЦН «Семья»
«Дом социальной реабилитации семей и детей «Борки»**

1. Общие положения

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

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, Федерального закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных", а также Федерального закона от 27.07.2006г. №149-ФЗ "Об информации, информационных технологиях и о защите информации".

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом директора Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. При заключении трудового договора лицо, поступающее на работу, предъявляет работодателю следующие документы:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний;
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям - при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

В отдельных случаях с учетом специфики работы может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

Для получения справок с места работы, дополнительных социальных льгот представляются дополнительные необходимые документы (свидетельство о рождении ребенка, свидетельство о браке, ИНН, справка МСЭ и т.д.)

2.3. Запрещается требовать от лица, поступающего на работу, документы, помимо предусмотренных Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

2.4. Состав персональных данных работника:

- Фамилия, имя, отчество;
- Дата рождения;
- Анкета;
- Автобиография;
- Паспортные данные;
- Адрес места регистрации/места жительства;
- Номера домашнего и сотового телефонов;
- Образование, специальность, сведения о курсах повышения квалификации, о наличии специальных знаний, о переподготовке работников, об аттестации работников;
- Профессия / квалификация;
- Семейное положение;
- Сведения о доходах, заработной плате работников;
- Сведения о стаже работы;
- ИНН;
- СНИЛС;
- Сведения о воинском учете для военнообязанных и лиц, подлежащих призыву на военную службу;
- Сведения о наличии (отсутствии) судимости;
- Занимаемая должность;
- Содержание трудового договора и дополнительных соглашений к нему;
- Содержание декларации, подаваемой в налоговую инспекцию;
- Приказы и копии приказов по личному составу;
- Табеля учета рабочего времени;
- Личные дела и трудовые книжки работников;
- Основания к приказам по личному составу;
- Сведения о служебных расследованиях;
- Сведения о результатах медицинского обследования;
- Медицинские книжки;
- Сведения о наличии инвалидности;
- Сведения о социальных льготах;
- Рекомендации, характеристики, сведения о наградах;
- Фотографии и иные сведения, относящиеся к персональным данным работника.

2.5. Персональные данные физических лиц содержатся в следующих ИСПДн: 1С: «Предприятие», 1С: «Зарплата и кадры», АЦК финансы, Интернет клиент, Крипто Про СР, СУФД-веб, АРМ генерация ключей, Континент АП.

2.6. Указанные в пп. 2.2, 2.4 сведения являются конфиденциальными и не подлежат разглашению иначе как по основаниям, предусмотренным законодательством РФ.

3. Создание, обработка и хранение персональных данных работника

3.1. Создание персональных данных работника.

Документы, содержащие персональные данные работника, создаются путем:

- а) копирования оригиналов (паспорт, документ об образовании, свидетельство ИНН, СНИЛС, военный билет, свидетельство о рождении ребенка, свидетельство о браке и др.);
- б) внесения сведений в учетные формы (на бумажных, электронных носителях и ИСПДн);
- в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, автобиография, согласие на обработку персональных данных, обязательство о неразглашении информации, медицинское заключение и пр.).

3.2. Для целей настоящего Положения используются следующие основные понятия:

- 1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2) информация - сведения (сообщения, данные) независимо от формы их представления;

3) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

4) 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;

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

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

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

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

9) 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;

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

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

12) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3.2.1. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов.

3.2.2. Обработка персональных данных работника осуществляется исключительно в целях:

- а) обеспечения соблюдения законов и иных нормативных правовых актов;
- б) содействия работникам в трудоустройстве;
- в) обеспечения личной безопасности работников;
- г) контроля количества и качества выполняемой работы;
- д) обеспечения сохранности имущества работника и работодателя.

3.2.3. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны.

3.2.4. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

- а) о целях получения персональных данных;
- б) о предполагаемых источниках и способах получения персональных данных;
- в) о характере подлежащих получению персональных данных;
- г) о последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.2.6. 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.

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

3.2.8. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств, в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

3.2.9. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

3.3. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы N Т-2, а также содержатся на электронных носителях информации и ИСПДн, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях.

3.4. Хранение персональных данных у лица ответственного за ведение кадрового делопроизводства и в бухгалтерии:

а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом шкафу, установленном на рабочем месте бухгалтера и лица ответственного за ведение кадрового делопроизводства;

б) персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК главного бухгалтера, бухгалтера и лица ответственного за ведение кадрового делопроизводства.

3.4.1. Персональные данные, включенные в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте лица ответственного за ведение кадрового делопроизводства.

3.4.2. Трудовые книжки хранятся в запертом металлическом сейфе, документы воинского учета, карточка формы N Т-2 хранятся в запертом металлическом шкафу.

3.4.3. Доступ к ПК строго ограничен кругом лиц, определенных в п. 6.1 настоящего Положения. Персональные данные, содержащиеся на бумажных носителях, после истечения установленного срока хранения, сдаются в архив.

4. Права и обязанности работника

4.1. Работник обязан:

- Передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ.

- Своевременно в разумный срок, сообщать работодателю об изменении своих персональных данных.

4.2. Работник имеет право:

- На полную информацию о своих персональных данных и обработке этих данных.

- На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством РФ.

- На определение своих представителей для защиты своих персональных данных.

- На доступ к медицинским данным с помощью медицинского специалиста по своему выбору.

- Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных Трудовым кодексом или иными федеральными законами. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

- Требовать об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

- Обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

5. Передача персональных данных

5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, предусмотренных Трудовым кодексом или иными федеральными законами;

- 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 конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом РФ и иными федеральными законами;

- осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, 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 РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

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

6. Доступ к персональным данным

6.1. Внутренний доступ (доступ внутри организации).

6.1.1. Право доступа к персональным данным сотрудника имеют:

- директор организации;

- 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.

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

6.2. Внешний доступ.

6.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные функциональные структуры:

- налоговые инспекции;

- правоохранительные органы;

- органы статистики;

- военкоматы;

- органы социального страхования;

- пенсионные фонды;

- подразделения муниципальных органов управления.

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

6.2.3. Организации, в которые сотрудник может осуществлять перечисление денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае подписания им согласия на обработку персональных данных.

6.2.4. Сведения об уволенном сотруднике могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии заявления работника.

7. Защита персональных данных

7.1. 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.

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

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

7.4. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

7.5. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для постороннего 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.

8. Порядок уничтожения, блокирования персональных данных

8.1. В случае выявления неправомерной обработки персональных данных при обращении Работника Работодатель обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Работнику, с момента такого обращения на период проверки.

8.2. В случае выявления неточных персональных данных при обращении Работника Работодатель обязан осуществить блокирование персональных данных, относящихся к этому Работнику, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы Работника или третьих лиц.

8.3. В случае подтверждения факта неточности персональных данных Работодатель на основании сведений, представленных Работником, или иных необходимых документов обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Работодателем, Работодатель в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных.

8.5. В случае если обеспечить правомерность обработки персональных данных невозможно, Работодатель в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

8.6. Об устранении допущенных нарушений или об уничтожении персональных данных Работодатель обязан уведомить Работника.

8.7. В случае достижения цели обработки персональных данных Работодатель обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не

превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено трудовым договором.

8.8. В случае отзыва Работником согласия на обработку его персональных данных Работодатель обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено трудовым договором.

8.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 8.4.-8.8. настоящего Положения, Работодатель осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

9. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными работника

9.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной ответственности. К данным лицам могут быть применены следующие дисциплинарные взыскания:

- а) замечание;
- б) выговор;
- в) предупреждение о неполном должностном соответствии;
- г) освобождение от занимаемой должности;
- д) увольнение.

9.2. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

9.3. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

9.4. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.