**Приложение № 2**

Согласовано: Утверждаю:

Председатель профсоюзного комитета Директор МБУ КЦСОН

МБУ КЦСОН

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Д.Синяева \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.В. Скоркина

**Положение о защите персональных данных работников**

**МБУ «Комплексный центр социального обслуживания населения»**

**Башмаковского района**

1. **Общие положения**

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты. Под работниками подразумеваются лица, заключившие трудовой договор с предприятием.

1.2. Основанием для разработки настоящего Положения являются: Конституция РФ, гл. 14 Трудового кодекса РФ, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", другие действующие нормативно-правовые акты РФ.

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

1.4. Настоящее Положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников. Все работники учреждения должны быть ознакомлены под расписку с данным Положением.

1. **Понятие и состав персональных данных**

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

2.2. В состав персональных данных работника входят:

2.2.1. Носители персональных данных
 Бумажные носители персональных данных:
- трудовая книжка;
- журналы учета трудовых книжек;
- журнал учета командировок;
- листки нетрудоспособности;
- материалы по учету рабочего времени;
- личная карточка Т-2;
- приказы по личному составу.
 Электронные носители персональных данных - база данных по учету работников предприятия.
2.2.2. Личное дело работника
 Перечень документов, содержащихся в личном деле работника при приеме на работу:
- копия паспорта;
- копия свидетельства о присвоении ИНН;
- копия страхового пенсионного свидетельства;
- копия военного билета (у военнообязанных);
- копия документов об образовании (в том числе и дополнительного образования, если работник представляет их при приеме на работу или это требуется при выполнении определенных трудовых функций);
- копия водительского удостоверения и документов на машину, если это требуется в связи с выполнением трудовой функции работника;
- медицинская справка о прохождении медицинского осмотра;
- трудовой договор;
- документы о прохождении обучения, испытательного срока;
- документы о составе семьи работника, необходимые для предоставления ему гарантий, связанных с выполнением семейных обязанностей;
- иные документы персонального учета, относящиеся к персональным данным работника.
- сведения о заработной плате сотрудника;

- сведения о социальных льготах;

- дополнительные соглашения;
- документы о повышении квалификации (письменные аттестации, дипломы, свидетельства и т.д.);
- документы о состоянии здоровья детей и других близких родственников, когда с наличием таких документов связано предоставление работнику каких либо гарантий и компенсаций;
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;
- документы о беременности работницы и возрасте детей для предоставления матери (отцу, другим родственникам) установленных законом условий труда, гарантий и компенсаций;
- иные документы персонального учета, относящиеся к изменениям персональных данных работника.

- копии отчетов, направляемые в органы статистики.

1. **Сбор и обработка, передача персональных данных**

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

**3.2**. Персональные данные работника следует получать у него самого. Работник обязан передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ. Своевременно сообщать работодателю об изменении своих персональных данных.
3.3. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только  с его письменного согласия.

3.5. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

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

3.6.1. 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, установленных федеральным законом;

- 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).

- 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.

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

3.6.3. Допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу, но только с согласия самого работника.

1. **Доступ к персональным данным**

**4.1.** Внутренний доступ (доступ внутри организации).

К обработке, передаче и хранению персональных данных работника могут иметь *доступ* следующие сотрудники:

- директор учреждения;

- инспектор по кадрам,

- работники бухгалтерии;

- заведующие отделениями,

- сам работник, носитель данных.

- другие сотрудники организации при выполнении ими своих служебных обязанностей.

**4.2**. Внешний доступ.

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

- налоговые инспекции;

- правоохранительные органы;

- органы статистики;

- страховые агентства;

- военкоматы;

- органы социального страхования;

- пенсионные фонды;

- подразделения муниципальных органов управления;

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

4.2.3. Организации, в которые 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.

4.2.4. Другие организации.

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

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

**4.3.** Должности, ответственные за сбор персональных данных -директор учреждения, инспектор отдела кадров, работники бухгалтерии.

Должности, ответственные за обработку персональных данных, - инспектор отдела кадров, работники бухгалтерии.

**5. Защита персональных данных**

5.1. 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.

5.2. 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.

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

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

5.4.1. Персональные данные на бумажных носителях хранятся в сейфе. При работе документы могут находиться на рабочих столах или в специальных папках только в течение рабочего дня. По окончании рабочего дня документы должны убираться в запирающиеся шкафы.

***5.5. «Внутренняя защита».***

5.5.1. 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 организации.

5.5.2. Для обеспечении 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 нарушения требований разрешительной системы доступа работниками подразделения;

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

- личные дела могут выдаваться на рабочие места только директору учреждения, работникам отдела кадров и бухгалтерии и в исключительных случаях- руководителю структурного подразделения. (например, при подготовке материалов для аттестации работника).

**5.6.** ***«Внешняя защита».***

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые 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.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, 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 учреждении.

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

- порядок приема, учета и контроля деятельности посетителей;

- пропускной режим организации;

- технические средства охраны, сигнализации;

- порядок охраны территории, зданий, помещений, транспортных средств.

5.6.4. По возможности персональные данные обезличиваются.

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

***5.7. Защита информации в информационных системах персональных данных***

5.7.1. При работе на персональных компьютерах, где находятся персональные данные работников, необходимо соблюдать ряд мер:

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

- ограничение доступа пользователей к информационным ресурсам;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;

- использование защищенных каналов связи.

**6. Ответственность за разглашение конфиденциальной информации,**

**связанной с персональными данными**

6.1 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.