УТВЕРЖДЕНО
Директор ГБСУСО МО
«Семейный центр имени А.И. Мещерякова»

_____ Г.К. Епифанова

Приказом от « 25 » ноября 2022 г. № 154

Положение о защите персональных данных работников Государственного бюджетного стационарного учреждения социального обслуживания Московской области «Семейный центр имени А.И. Мещерякова»

1. Общие положения

1.1. Настоящее Положение о защите персональных данных работников Государственного бюджетного стационарного учреждения социального обслуживания Московской области «Семейный центр имени А.И. Мещерякова» (далее - Учреждение) разработано в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации", Трудовым кодексом Российской Федерации, другими действующими нормативными правовыми актами Российской Федерации (далее - Положение).
1.2. Цель настоящего Положения - защита персональных данных работников Учреждения от несанкционированного доступа и разглашения. Персональные данные работников всегда являются конфиденциальной, строго охраняемой информацией, в соответствии с действующим законодательством Российской Федерации.
1.3. Положение устанавливает порядок защиты информации, содержащей сведения, отнесенные к персональным данным работников Учреждения (далее – персональные данные). Под работниками подразумеваются лица, заключившие трудовой договор с Учреждением.
1.4. Положение и изменения к нему утверждаются директором Учреждения и вводятся его приказом. Все работники Учреждения должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

2. Понятие и состав персональных данных работника

2.1. Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу.

2.2. Состав персональных данных работника:
- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии), дата и место их изменения (в случае изменения);
- дата (число, месяц, год) и место рождения;
- сведения о документе, удостоверяющем личность - вид, серия, номер, наименование органа, выдавшего его, дата выдачи;

- адрес и дата регистрации по месту жительства (месту пребывания),
- адрес фактического проживания;
- сведения о гражданстве;
- сведения об образовании;
- сведения о трудовой деятельности, трудовом и общем стаже, трудовом договоре;
- сведения о предыдущем месте работы;
- сведения о семейном положении, составе семьи, наличии детей, родственных связей;
- сведения о воинском учете;
- сведения о социальных льготах;
- сведения о занимаемой должности;
- сведения о размере заработной платы;
- сведения о наличии судимостей;
- идентификационный номер налогоплательщика (ИНН),
- страховой номер индивидуального лицевого счета (СНИЛС);
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографическое, видео- и цифровое изображение;
- сведения о принадлежности лица к конкретной нации, этнической группе, расе;
- сведения о привычках и увлечениях, в том числе вредных (алкоголь, наркотики и др.);
- сведения о религиозных и политических убеждениях (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);
- сведения о финансовом положении (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);
- сведения о деловых и иных личных качествах субъекта, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека.

Из указанного списка работодатель (Учреждение) вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.3. Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет (75 лет — если документы оформлены до 01 января 2003 года) срока хранения, если иное не определено законом.

3. Доступ к персональным данным работников

3.1. Внутренний доступ (доступ внутри Учреждения).

Право доступа к персональным данным работников имеют:

- руководитель (директор) Учреждения - доступ к личным данным всех работников Учреждения;
- руководитель отдела кадров, специалист по кадрам – доступ, а также сбор, обработка, хранение, передачу персональных данных всех работников Учреждения;
- руководители структурных подразделений по направлению деятельности - заместители директора, заведующий отделением учебно-воспитательной работы заведующий медицинским подразделением - доступ к личным данным только работников своего подразделения;
- при переводе из одного структурного подразделения в другое доступ к персональным данным работника может иметь руководитель нового подразделения;

- работники бухгалтерии - главный бухгалтер, заместитель главного бухгалтера, бухгалтер, экономист - к тем персональным данным всех работников Учреждения, которые необходимы для выполнения конкретных функций;
- старшая медицинская сестра, медицинская сестра диетическая, специалист в сфере закупок, юрисконсульт, заведующий хозяйством, комендант, начальник гаража, специалист по охране труда, электроник, библиотекарь, секретарь, секретарь учебной части. - к тем персональным данным всех работников Учреждения, которые необходимы для выполнения конкретных функций;
- сам работник, носитель данных.

3.2. Внешний доступ.

Учреждение вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

Перед передачей персональных данных Учреждение должно предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено.

3.3. Не требуется согласие работника на передачу персональных данных:
- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Фонд социального страхования Российской Федерации, Пенсионный фонд Российской Федерации в объеме, предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов, включая в целях контроля за соблюдением трудового законодательства работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников.

3.4. Другие организации.

Сведения о работнике *(в том числе уволенном)* могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

3.5. Родственники и члены семей.

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

4. Защита персональных данных работников

4.1. В целях обеспечения сохранности и конфиденциальности персональных данных работников организации все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками отдела кадров, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

4.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Учреждения в том объеме,

который позволяет не разглашать излишний объем персональных данных о работниках Учреждения.
4.3. Передача информации, содержащей сведения о персональных данных работника организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.
4.4. Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа. Выдача ключей от помещений, в которых находятся указанные шкафы (сейфы), осуществляется под подпись.
4.5. Персональные компьютеры, в которых содержатся персональные данные работников, должны быть защищены паролями доступа.
4.6. С целью защиты персональных данных работников в Учреждении приказами директора назначается (утверждаются):
- работник, ответственный за организацию обработки персональных данных;
- форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.
4.7. Работники, которые занимают должности, предусматривающие сбор, обработку, хранение, передачу персональных данных работников и (или) доступ к ним, обязаны не разглашать указанные персональные данные.
4.8. В Учреждении используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
4.9. Работники Учреждения, обрабатывающие персональные данные, периодически проходят обучение требованиям законодательства в области персональных данных.
4.10. Работники Учреждения, ведущие сбор, обработку, хранение и передачу персональных данных, а также, имеющие право на внутренний доступ к ним, обязаны сообщать о любых случаях несанкционированного доступа к персональным данным.
4.11. В Учреждении проводятся внутренние расследования в следующих ситуациях:
- при неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- в иных случаях, предусмотренных законодательством в области персональных данных.
4.12. Работник, ответственный за организацию обработки персональных данных, осуществляет внутренний контроль:
- за соблюдением работниками, уполномоченными на обработку персональных данных, а также имеющих право доступа к ним, в соответствии с п. 3.1. настоящего Положения, требований законодательства в области персональных данных, локальных нормативных актов;
- соответствием указанных актов, требованиям законодательства в области персональных данных.
Внутренний контроль проходит в виде внутренних проверок.
4.12.1. Внутренние проверки осуществляются по решению директора Учреждения. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде.
4.12.2. По итогам внутренней проверки оформляется докладная записка на имя директора. В случае выявления нарушений в документе приводятся перечень мероприятий по их устранению и соответствующие сроки.
4.13. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).
4.13.1. В случае инцидента Учреждение в течение 24 часов уведомляет Роскомнадзор:
- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) персональных данных;
- принятых мерах по устранению последствий инцидента;

- представителе Учреждения, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

4.13.2. В течение 72 часов Учреждение обязано сделать следующее:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии);
- осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

4.14. В случае предоставления субъектом персональных данных (его представителем) подтвержденной информации о том, что персональные данные являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. Учреждение уведомляет в письменном виде субъекта персональных данных (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы персональные данные.

4.15. Учреждение уведомляет субъекта персональных данных (его представителя) об устранении нарушений в части неправомерной обработки персональных данных. Уведомляется также Роскомнадзор, если он направил обращение субъекта персональных данных (его представителя) либо сам сделал запрос.

4.15.1. В случае уничтожения персональных данных, которые неправомерно обрабатывались, уведомление направляется в соответствии с п. 4.15 Положения.

4.16. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, Учреждение уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Учреждение уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

5. Ответственность за разглашение информации, связанной с персональными данными работника

5.1. Лица, виновные в нарушении норм, регулирующих защиту персональных данных работника, несут дисциплинарную и материальную ответственность в порядке, установленном Трудовым кодексом Российской Федерации, а также административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.