«УТВЕРЖДАЮ»:
ГКУЗ КО Главный врач
ГКУЗ КО А-С ДРС «Маленькая страна»
_____ Т.Н. Акатьева
«15» января 2014 г

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников ГКУЗ КО «Анжеро-Судженский дом ребенка специализированный «Маленькая страна»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обработке и защите персональных данных в ГКУЗ КО А-С ДРС «Маленькая страна» (далее – Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в ГКУЗ КО А-С ДРС «Маленькая страна» (далее – Учреждение).

1.2. Настоящее Положение определяет политику Учреждения как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации (далее – Трудовой кодекс Российской Федерации), Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.05.2003 № 58-ФЗ «О системе государственной службы Российской Федерации» (далее – Федеральный закон «О системе государственной службы Российской Федерации»), Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее – Федеральный закон «О государственной гражданской службе Российской Федерации»), Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции» (далее – Федеральный закон «О противодействии коррупции»), Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – Федеральный закон «Об организации предоставления государственных и муниципальных услуг»), Федеральным законом от 02.09.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»), Федеральным законом от 07.07.2003 № 126-ФЗ «О связи», Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (далее – Федеральный закон «О

лицензировании отдельных видов деятельности»), Законом Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации» (далее – Закон Российской Федерации «О средствах массовой информации»), Указом Президента Российской Федерации от 30 мая 2005г. №609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», постановлением Правительства Российской Федерации от 16 марта 2009г. №228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций», постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 6 июля 2008г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 10 сентября 2009г. №23 «О порядке ввода в эксплуатацию отделанных государственных информационных систем».

1.4. Обработка персональных данных в ГКУЗ КО А-С ДРС «Маленькая страна» осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

II. 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 его жизни, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

2.1.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2.1.2. число, месяц, год рождения;

2.1.3. место рождения;

2.1.4. вид, серия, номер документа, удостоверяющего личность,

наименование органа, выдавшего его, дата выдачи;

2.1.5. адрес места жительства (адрес регистрации, фактического проживания);

2.1.6. номер контактного телефона или сведения о других способах связи;

2.1.7. реквизиты страхового свидетельства государственного пенсионного страхования;

2.1.8. идентификационный номер налогоплательщика;

2.1.9. реквизиты страхового медицинского полиса обязательного медицинского страхования;

2.1.10. реквизиты свидетельства государственной регистрации актов гражданского состояния;

2.1.11. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

2.1.12. сведения о трудовой деятельности;

2.1.13. сведения о воинском учете и реквизиты документов воинского учета;

2.1.14. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

2.1.15. сведения об ученой степени;

2.1.16. информация о владении иностранными языками, степень владения;

2.1.17. фотография;

2.1.18. информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;

2.1.19. информация о наличии или отсутствии судимости;

2.1.20. информация об оформленных допусках к государственной тайне;

2.1.21. государственные награды, иные награды и знаки отличия;

2.1.22. сведения о профессиональной переподготовке и (или) повышении квалификации;

2.1.23. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

2.1.24. сведения о доходах, об имуществе и обязательствах имущественного характера;

2.1.25. номер расчетного счета;

2.1.26. номер банковской карты;

2.1.27. иные персональные данные.

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

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

2.4. 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, и который вступил (стал работником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных, кроме случаев, когда передача персональных данных обусловлена действующим законодательством.

2.5. Держателем персональных данных является работодатель, которому работник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.6. 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 знания персональных данных работников или связана с обработкой этих данных.

2.7. 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 работника 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 работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. Все персональные данные работника получаются у него самого. Если персональные данные о работнике 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 также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.4. Не допускается получение и обработка персональных данных работника 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 РФ.

3.5. При принятии решений относительно работника 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 ст. 24 Конституции Российской Федерации возможно получение и обработка данных о частной жизни работника только с его письменного согласия.

3.7. Пакет анкетно-биографических и иных характеризующих его материалов (далее пакет) работника формируется после издания приказа о его приеме на работу. Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные работника в порядке, отражающем процесс приема на работу.

3.8. Все документы хранятся в папках в алфавитном порядке фамилий работников.

3.9. Пакет пополняется на протяжении всей трудовой деятельности работника в данной организации. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

3.10. Работник службы кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу лица документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

3.11. 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.

3.12. При обработке персональных данных работников работодатель в лице руководителя инспекции вправе определять способы обработки, документирования, хранения и защиты персональных данных работников общества на базе современных информационных технологий.

3.13. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.
- Работник 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 работника, за исключением случаев, предусмотренных действующим законодательством;
- определение своих представителей для защиты своих персональных данных;
- доступ к относящимся к нему медицинским данным с помощью медицинского специалиста 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 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;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, 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 работником непосредственно держателю этих данных и потребителям внутри инспекции исключительно для обработки и использования в работе.

4.2. **Внешний доступ.** К числу массовых потребителей персональных данных вне ГКУЗ КО А-С ДРС «Маленькая страна» относятся государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- органы прокуратуры;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

4.3. **Внутренний доступ.** Внутри ГКУЗ КО А-С ДРС «Маленькая страна» к разряду потребителей персональных данных относятся работники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- работники службы кадров;
- работники бухгалтерии;
- начальники структурных подразделений.

4.4. В кадровой службе хранятся личные карточки работников, работающих в настоящее время. Личные карточки располагаются по структурным подразделениям.

4.5. После увольнения документы по личному составу передаются на хранение в установленном порядке.

V. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

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

5.1.1. **при передаче 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 работника потребителям (в том числе и в коммерческих целях) за пределы инспекции работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных действующим законодательством;
- ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения руководителя инспекции 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.

5.1.2. **при передаче внутреннему потребителю:** работодатель вправе разрешать доступ к персональным данным работников. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных работника.

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 инспекции.

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, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами инспекции. Для 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 работниками 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 банк персональных данных работников;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только руководителю инспекции и, в исключительных случаях, по письменному разрешению руководителя инспекции, заместителю руководителя или начальнику структурного подразделения;
- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

6.5. **«Внешняя защита»**. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся 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 общества, 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 в службе кадров.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

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

VII. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

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

Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый работник ГКУЗ КО А-С ДРС «Маленькая страна», получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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.

Специалист по кадрам  Е.А. Иноземцева