УТВЕРЖДАЮ

Директор ГБУСОВО «Копнинский ПНИ»

_____Т.В. Королёва

«11» января 2016 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в ГБУСОВО «Копнинский ПНИ»

2016г.

СОДЕРЖАНИЕ

1. Общие положения

1.1. Целью данного Положения является определение порядка обработки персональных данных в ГБУСОВО «Копнинский ПНИ» (далее - Организация); обеспечение защиты прав и свобод работников и обслуживаемых граждан (далее - Обеспечиваемые) Организации при обработке их персональных данных (далее - ПДн), а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ и устанавливает единый порядок обработки персональных данных в Организации.

1.3. Настоящее Положение утверждается и вводится в действие приказом Генерального директора и является обязательным для исполнения всеми работниками Организации, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. 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. Состав персональных данных работника определён в Перечне персональных данных в ГБУСОВО «Копнинский ПНИ».

3. Обработка персональных данных

3.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению №1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Владимирской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;

- после принятия необходимых мер по защите персональных данных.

3.2. Приказом руководителя назначается сотрудник, ответственный за организацию обработки персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

3.3. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно приложению №2 к настоящему Положению.

3.4. Запрещается:

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;

- осуществлять ввод персональных данных под диктовку.

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

3.5.1. 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, обеспечения личной безопасности

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

3.5.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.5.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.5.4. Персональные данные работника следует получать у него самого. 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 также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.5.5. 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.

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

3.6.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их

социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.7. Передача персональных данных работника или обслуживаемого Организации возможна только с согласия субъекта персональных данных или в случаях, прямо предусмотренных законодательством.

3.7.1. 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 конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- лица, допущенные к обработке персональных данных работников, 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.

3.7.2. 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.

3.7.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации 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 федеральным законом.

3.7.4. В случае, если Организации оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным работников и (или) обслуживаемых Организации, то соответствующие данные предоставляются Организацией только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работника и (или) обслуживаемого.

3.8 При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Лицо, ответственное за организацию обработки ПДн, а также лица, обрабатывающие ПДн, обеспечивают своевременное удаление или уточнение неполных или неточных данных.

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

3.9.1. Требуется обеспечивать раздельное хранение ПДн с несовместимыми целями хранения.

3.9.2. Места хранения материальных носителей персональных данных должны быть определены в отдельном локальном нормативно-правовом акте Организации.

3.10. Срок обработки ПДн определён до момента достижения целей обработки. Срок последующего хранения ПДн определяется законодательством Российской Федерации и приведён в Перечне персональных данных.

3.11. Порядок уничтожения персональных данных.

3.11.1. Ответственным за организацию обработки ПДн осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения и подлежащих уничтожению.

3.11.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии, состав которой утверждается приказом директора.

3.11.3. По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел; дела проверяются на их комплектность, акт подписывается председателем и членами комиссии и утверждается директором.

3.11.4. Уничтожение документов, содержащих персональные данные, производится членами комиссии путем сжигания или аппаратного измельчения.

3.11.5. По окончании процедуры уничтожения, Ответственным за организацию обработки ПДн составляется соответствующий акт об уничтожении документов, содержащих персональные данные.

3.11.6. Уничтожение персональных данных на электронных носителях производится путем программного удаления необходимой информации, исключающего восстановление уничтоженных ПДн.

4. Доступ к персональным данным

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным работника имеют:

- сам работник, носитель данных.

- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Право доступа к персональным данным обслуживаемых имеют только лица, допущенные к обработке данной информации, в связи с должностными обязанностями.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных работников 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 работник 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 нотариально заверенного заявления работника.

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

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (согласно УК РФ).

5. Защита персональных данных

5.1. В целях обеспечения защиты персональных данных в Организации создаётся и обслуживается система защиты информации, которая представляет собой совокупность правовых, организационных, программно-технический и физических мер защиты информации.

5.2. Под угрозой безопасности персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление дестабилизирующего воздействия на защищаемую информацию.

5.3. 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 компании.

5.4. Защита от внутренних нарушителей.

5.4.1. Главной причиной несанкционированного доступа к персональным данным являются, как правило, умышленные или непреднамеренные действия персонала, работающего с документами и базами данных.

5.4.2. Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и утверждение состава работников, функциональные обязанности которых требуют работы с персональными данными;

- строгое избирательное и обоснованное разграничение прав доступа персонала к конфиденциальным сведениям;

- 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, в том числе могут применяться инженерно-технические средства защиты информации (СКУД), жалюзи и решётки на окнах, сейфы и металлические шкафы;

- определение и утверждение состава работников, имеющих право доступа (входа) в помещения, в котором находятся элементы ИСПДн;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

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

5.5. Защита от внешних нарушителей.

5.5.1. 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.

5.5.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Организации, 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.

5.5.3. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер, в том числе могут быть:

- соблюдение порядка приема, учета и контроля деятельности посетителей;

- пропускной режим организации;

- использование технических средств охраны и сигнализации;

- использование технических средств защиты информации;

- соблюдение порядка охраны территории, зданий, помещений, транспортных средств;

- выполнения требований по защите информации при интервьюировании и собеседованиях.

6. Права и обязанности субъекта персональных данных

6.1. Все работники Организации должны быть ознакомлены с настоящим Положением под роспись.

6.2. Работники и обслуживаемые имеют 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.

6.3. Работники и обслуживаемые обязаны:

- передавать Организации или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен

Трудовым кодексом РФ и (или) законодательством о социальной защите населения.

- своевременно сообщать Организации об изменении своих персональных данных.

- соблюдать конфиденциальность персональных данных, ставших известными работнику во время исполнения своих должностных обязанностей.

6.4. Работники ставят работодателя 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.

7. Ответственность за разглашение информации, содержащей персональные данные

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

7.2 Работники Организации, допущенные к обработке ПДн, в обязательном порядке подписывают обязательства о неразглашении информации, содержащей персональные данные, по форме, приведённой в приложении №2 к данному документу

7.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

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

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

7.6. 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.

7.6.1. 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.

7.6.2. Должностные лица, в обязанность которых входит обработка 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.

7.6.3. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего 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 наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.7. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.