Калямина Ирина Петровна
Подписано цифровой подписью: Калямина Ирина Петровна
Дата: 2021.02.18 18:59:00 +05'00'

Утверждено
приказом МАДОУ «Чебурашка»
от «01» октября 2015г. № 193

ПОЛОЖЕНИЕ
об организации работы с персональными данными работников МАДОУ «Чебурашка»

1. Общие положения

1.1. Положение об организации работы с персональными данными работников (далее по тексту – Положение) Муниципального автономного дошкольного образовательного учреждения города Когалыма «Чебурашка» (далее по тексту – Учреждение) разработано с целью защиты персональных данных работников Учреждения, от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании Конституции Российской Федерации, Федерального закона от 27 июля 2006 №152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

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 заведующего Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

1.5. Срок данного положения не ограничен. Положение действует до принятия нового.

2. Понятие и состав персональных данных

2.1. Персональные данные работника Учреждения - 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:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;

- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- информация о состоянии здоровья Работника (в том числе сведения об инвалидности и т.п.);
- ИНН;
- документы, содержащие сведения, необходимые для предоставления Работнику гарантий и компенсаций, установленных действующим законодательством (документы о составе семьи; документы о состоянии здоровья детей; документы, подтверждающие дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (донорстве, нахождения в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.); документы о беременности Работницы; документы о возрасте малолетних детей).

2.3. Все персональные данные о работнике администрация может получить только от него самого. Работник принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие оформляется в письменной форме (в соответствии с приложением 1 к Положению о порядке разработки и защите персональных данных в МАДОУ «Чебурашка»), которое хранится у оператора персональных данных в течение срока, указанного в Согласии. В случаях, когда администрация может получить необходимые персональные данные Работника только у третьего лица, администрация должна уведомить об этом Работника заранее и получить от него письменное согласие.

2.4. Администрация обязана сообщить Работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа Работника дать письменное согласие на их получение.

2.5. Документы, указанные в п. 2.2. настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных.

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

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

3.2.1. 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;

3.2.2. при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами;

3.2.3. право на обработку персональных данных работников Учреждения имеют:

- специалист отдела кадров;
- главный бухгалтер;
- экономист;
- специалист расчетного отдела;
- заведующий;
- документовед;
- заместитель заведующего;
- старший воспитатель;
- специалист по охране труда (в рамках своей компетенции).

3.3.Права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работников Учреждения, определяются трудовыми договорами и должностными инструкциями.

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

3.5.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.

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

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

3.7.1. 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;

3.7.2. не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

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

3.7.4. разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по Учреждению, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

3.7.5. не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

3.7.6. 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.

3.8.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.

3.9.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.

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

3.11.Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

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

3.13.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. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

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

4.1.1. Право доступа к персональным данным сотрудника имеют:

- заведующий Учреждения;
- заместитель заведующего;

- старший воспитатель (в пределах своей компетенции);
- специалист по охране труда (в пределах своей компетенции);
- документовед;
- сам работник, носитель данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом заведующего Учреждения.

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.
- 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 Учреждение с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ).

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 представляет собой регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете обеспечивающий достаточную безопасность информации в процессе деятельности Учреждения.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств, в порядке, установленном федеральными законами.

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 обеспечения 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;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- организация порядка уничтожения информации;
- воспитательная и разъяснительная работа с сотрудниками Учреждения по предупреждению утраты сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только начальнику, заведующим ДОУ.

5.5.3. Защита персональных данных сотрудника на электронных носителях. Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается работнику, имеющему доступ к персональным данным.

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.

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

- порядок приема, учета и контроля деятельности посетителей;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников (в соответствии с приложением 2 к Положению о порядке разработки и защите персональных данных в МАДОУ «Чебурашка»).

5.8. По возможности персональные данные могут быть обезличены.

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

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

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

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет 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.

6.4. 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.

6.5. 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.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

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

7.2. 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.

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

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

7.5. 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:

7.5.1. 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;

7.5.2. должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом;

7.5.3. 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;

7.5.4. 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.

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