

П Р А В И Л А

обработки персональных данных в МБДОУ детского сада «Теремок»

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в МБДОУ детского сада «Теремок» (далее – Правила) разработаны в соответствии Федеральным законом от 27.07.2006 г. № 152 – ФЗ «О персональных данных, постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении Перечня мер, направленных на обеспечение обязанностей, предусмотренных Федеральным законом «О персональных данных» постановлением Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящие Правила устанавливают:

- ✓ порядок определения цели обработки персональных данных;
- ✓ процедуры, определяющие для каждой цели обработки данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются;
- ✓ сроки обработки и хранения обрабатываемых персональных данных;
- ✓ порядок обработки, хранения, распространения, блокирования, использования, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований персональных данных;
- ✓ правила работы с обезличенными данными;
- ✓ процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных;
- ✓ правила рассмотрения запросов субъектов персональных данных или их представителей;
- ✓ правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных законодательством.

1.3. МБДОУ детский сад «Теремок» самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку персональных данных, а также

определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия, совершаемые с персональными данными.

Понятия и определения используются в значениях, определенных Федеральным законом от 27.07.2006 г. № 152 – ФЗ « О персональных данных» и Федеральным законом от 27.07.2006 г. № 149 – ФЗ «Об информатизации, информационных технологиях и о защите информации», либо их значение дается по тексту.

1.4. Обработка персональных данных должна:

- ✓ осуществляться в соответствии с действующим законодательством;
- ✓ ограничиваться достижением конкретных, заранее определенных и законных целей.

1.5. Не допускается:

- ✓ обработка персональных данных, не совместимая с целями сбора персональных данных;
- ✓ объединение баз данных, содержащих персональные данные, которые осуществляются в целях, не совместимых между собой.

1.6. При обработке персональных данных должны быть обеспечены точность персональных данных, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

2. 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. К персональным данным относятся:

- ✓ фамилия, имя, отчество (в том числе предыдущие фамилия, имена и (или) отчества в случае их изменения);
- ✓ число, месяц, год рождения;
- ✓ место рождения;
- ✓ информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- ✓ вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- ✓ адрес места жительства (адрес регистрации, фактического проживания);
- ✓ номер контактного телефона или сведения о других способах связи;
- ✓ реквизиты страхового свидетельства государственного пенсионного страхования;
- ✓ идентификационный номер налогоплательщика;
- ✓ реквизиты страхового полиса обязательного медицинского страхования;
- ✓ семейное положение, состав семьи и сведения о близких родственниках;

- ✓ сведения о трудовой деятельности;
- ✓ сведения о воинском учете и реквизиты документов воинского учета;
- ✓ сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- ✓ медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на работу);
- ✓ фотография;
- ✓ информация о наличии или отсутствии судимости;
- ✓ дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- ✓ копии отчетов, направляемые в органы статистики.

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

3.2.4. 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 так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2.5. 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.

3.2.6. 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.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- ✓ бухгалтерии;
- ✓ воспитатель МБДОУ детского сада «Теремок»;
- ✓ юрист управления образования, по делам молодежи и спорта.

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

3.4.1. 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.

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

3.5.1. 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). Данное положение не

распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- ✓ разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным в Положении о разграничении прав доступа к персональным данным, 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.

3.5.2. 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.

3.5.3. 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.

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

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

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

3.9. 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. Получение персональных данных

4.1. Субъект персональных данных принимает решение о предоставлении его персональных данных, а в случаях, предусмотренных федеральным законом, дает согласие на обработку своих персональных данных. Субъект персональных данных принимает решение и дает согласие свободно, своей волей и в своем интересе.

Типовая форма согласия субъекта на обработку персональных данных представлена в Приложении № 1 к настоящим Правилам.

4.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

4.3. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных. Типовая форма согласия субъекта на обработку персональных данных подопечного представлена в Приложении № 2 к настоящим Правилам.

4.4. В случае отказа субъекта персональных данных предоставить свои персональные данные, если предоставление персональных данных является обязательным в соответствии с Федеральным законом от 27.07.2006 г. № 152 – ФЗ «О персональных данных», лицо, ответственное за предоставление (осуществление) функции, обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные приведена в Приложении № 3 к настоящим Правилам.

4.5. 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;

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

4.7. 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 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. (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 жестко регламентированный и динамически 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 персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. Защита от внутренних нарушителей.

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;
- ✓ 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.

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Защита персональных данных сотрудника на электронных носителях осуществляется в соответствии с Инструкцией по обеспечению безопасности рабочих мест обработки персональных данных.

5.6. Защита от внешних нарушителей.

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 Муниципального бюджетного дошкольного образовательного учреждения детский сад «Геремок», 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:

- ✓ соблюдение порядка приема, учета и контроля деятельности посетителей;
- ✓ пропускной режим организации;
- ✓ использование технических средств защиты информации (установление паролей на компьютерах);
- ✓ соблюдение порядка охраны территории, зданий, помещений;
- ✓ выполнения требований по защите информации при интервьюировании и собеседованиях.

6. Права и обязанности работника

6.1. Все работники должны быть ознакомлены с настоящими Правилами под роспись.

6.2. 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.

6.3. 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.
- ✓ соблюдать конфиденциальность персональных данных других работников, ставших ему известными 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 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 МБДОУ детского сада «Теремок», 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 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.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

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 наказываются 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.