

**1. Общие положения.**

1.1. Целью положения об обработке персональных данных работников (далее — Положение) является защита персональных данных работников МБДОУ д/с «Теремок» Зерноградского района от несанкционированного доступа, неправомерного их использования или утраты, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение разработано в соответствии со статьями 85-90 Трудового Кодекса Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Правилами внутреннего трудового распорядка ДОУ.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Положение вступает в силу с момента утверждения его заведующим МБДОУ д/с «Теремок» Зерноградского района и действует бессрочно, до замены его новым положением.

1.3.2. Все изменения в Положения вносятся соответствующим приказом.

I .4. Все работники ДОУ должны быть ознакомлены с настоящим Положением под подпись.

1.5. Режим конфиденциальности персональных данных снимается в случае их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии, если иное не определено законом.

**2. Основные понятия.**

2.1. Для целей настоящего Положения используются следующие основные понятия

— персональные данные работника — любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

— обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников;

— конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

— распространение персональных данных — действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;

— использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Общества в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

— блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

— уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;

— обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

— общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

— информация — сведения (сообщения, данные) независимо от формы их представления.

— документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

**3. Состав персональных данных работников.**

З. 1. В состав персональных данных работников ДОУ 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; — сведения о социальных льготах;

— специиьность,

— занимаемая должность;

— наличие (отсутствие) судимостей;

— адрес места жительства:

— домашний телефон;

— место работы или учебы членов семьи и родственников;

— содержание трудового договора;

— состав декларируемых сведений о наличии материальных ценностей;

— содержание декларации подаваемой в налоговую инспекцию;

— 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.

3.2. Данные документы являются конфиденциальными, при этом, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

1. **Обработка персональных данных.**

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

4.1.1.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.

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

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

4.1.1. 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 и последствиях отказа работника дать письменное согласие на их получение;

4.1.2. 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.

4.1.3. 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.

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

— Бухгалтерии;

— Отдела персонала;

— Отдела информационных технологий.

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

4.3.1. 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,

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

4.3.3. 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 приказом по организации, 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.

4.4.4. 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.

4.4.5. 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.

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

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

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

4.8. 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.

1. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в ДОУ при его приеме, переводе и увольнении.
   1. Информация представляемая работником при поступлении на работу в ДОУ, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо поступающее на работу, предъявляет работодателю:

— паспорт гражданина Российской Федерации;

— трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

— страховое свидетельство государственного пенсионного страхования;

— документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;

— документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;

— свидетельство о присвоении ИНН.

* 1. При оформлении работника в МБДОУ д/с «Теремок» Зерноградского района заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:
  2. — общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

— сведения о воинском учете;

— данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

— сведения о переводах на другую работу;

— сведения об аттестации;

— сведения о повышении квалификации;

— сведения о профессиональной переподготовке;

— сведения о наградах (поощрениях), почетных званиях;

— сведения об отпусках;

— сведения о социальных гарантиях;

— сведения о месте жительства и контактных телефонах.

5.4. В отделе персонала Общества создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

5.4.1. Документы содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу, дела, содержащие материалы аттестации работников; служебных расследований; справочно информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Организации. руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

5.4.2. Документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства ДОУ); документы по планированию, учету, анализу.

1. Доступ к персональным данным.
   1. Внутренний доступ (доступ внутри ДОУ),
      1. Право доступа к персональным данным сотрудника имеют:

- Заведующий МБДОУ д/с «Теремок» Зерноградского района — при переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника может иметь руководитель нового подразделения;

— сам работник, носитель данных.

— другие сотрудники организации при выполнении ими своих служебных обязанностей.

* 1. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом заведующего МБДОУ д/с «Теремок» Зерноградского района.
  2. Внешний доступ.
     1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

— налоговые инспекции;

— правоохранительные органы;

— органы статистики;

— военкоматы;

— органы социального страхования;

— пенсионные фонды;

— подразделения муниципальных органов управления;

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

6.3.3. 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.

6.3.4.Сведения о работающем сотруднике или уже уволенном могут быть представлены другой организацией только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

6.3.5. Персональные данные сотрудника могут быть представлены родственникам или членам его семьи ТОЛЬКО с письменного разрешения самого сотрудника.

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

1. Защита персональных данных
   1. 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.
   2. Защита персональных данных работника от неправомерного их использования или утраты. должна быть обеспечена Обществом за счет его средств в порядке, установленном федеральным законом.
   3. Внутренняя защита.

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

— ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным сотрудников.

— 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;

7.3.2. Защита персональных данных сотрудников на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны иметь ограниченный доступ (только для сотрудников отдела персонала и директора по информационным технологиям).

7.4. Внешняя защита,

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

— порядок приема, учета и контроля деятельности посетителей;

— пропускной режим организации;

— учет и порядок выдачи пропусков;

— технические средства охраны (электронный ключ, сигнализации);

— порядок охраны территории, зданий, помещений, транспортных средств;

7.5. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные работников.

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

8. Права и обязанности работника.

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

8.2 В целях защиты персональных данных, хранящяяся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных данных;

— получать свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные.

— персональные данные оценочного характера дополнить заявлением, содержащим его собственную точку зрения;

— определять своих представителей для защиты своих персональных данных;

— на сохранение и защиту своей личной жизни и семейной тайны.

8.3. Работник обязан передавать Обществу комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым Кодексом РФ, а также своевременно сообщать об изменениях своих персональных данных.

8.4. Работники ставят Общество 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.

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

9.1. Руководитель разрешающий доступ сотрудника к конфиденциальному документу, несет персональную Ответственность за данное разрешение.

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

9.3. 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.