УТВЕРЖДАЮ
Заведующий МБДОУ
д/с № 3 «Звездочка»
_____ Ф.Э. Нугаева
«01» сентября 2016 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ МБДОУ д/с №3 «Звездочка»

АНАПА
2016 год

СОДЕРЖАНИЕ:

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Цель данного Положения - защита персональных данных сотрудников от несанкционированного доступа, неправомерного использования или утраты.

1.2. Настоящее **Положение** устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников организации. Сотрудниками считаются лица, работающие в организации по трудовому договору. Положение устанавливает порядок использования персональных данных сотрудников в служебных целях.

1.3. Сбор, хранение, использование и распространение информации о частной жизни сотрудника без письменного его согласия не **допускается.** Персональные данные относятся к категории **конфиденциальной** информации.

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

1.5. Настоящее Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции РФ, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии с главой 14 Трудового кодекса РФ «Защита персональных данных работника», ст. 68, 81 ТК РФ.

1.6. 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.

1.7. 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.

1.8. Неправомерность деятельности организации по сбору персональных данных может быть установлена только в судебном порядке по требованию сотрудника в соответствии с законами РФ.

1.9. Настоящее Положение утверждается директором МБДОУ д/с №3 «Звездочка» и является обязательным для исполнения сотрудниками, имеющими доступ к персональным данным. Все сотрудники организации должны быть письменно под роспись ознакомлены с настоящим Положением.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ.

2.1. Персональные данные сотрудника – информация, необходимая организации в связи с трудовыми отношениями и касающиеся конкретного сотрудника (ст.85 ТК РФ), а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность, служебные сведения, а также иные сведения, связанные с профессиональной деятельностью сотрудника, в том числе сведения о поощрениях и о дисциплинарных взысканиях.

2.2. **Состав** персональных данных сотрудника:

- анкетные и биографические данные (карточка Т-2, автобиография, личный листок по учёту кадров);

- образование (документ об образовании);

- сведения о трудовом и общем стаже (трудовая книжка);

- сведения о составе семьи (свидетельство о браке, рождении детей и т.д.);

- паспортные данные (паспорт);

- сведения о воинском учете (военный билет);

- сведения о заработной плате сотрудника;

- сведения о социальных льготах;

- информация страхового свидетельства государственного пенсионного страхования;

- информация свидетельства о постановке на учёт в налоговый орган и присвоения ИНН;

- специальность (документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки);

- 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;

- сведения из заключения медицинской комиссии (медицинские книжки);

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

3. ОБЯЗАННОСТИ И ПРАВА СОТРУДНИКА.

3.1. Обязанности сотрудника.

3.1.1. Передавать организации или её представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

3.1.2. Своевременно сообщать организации об изменении своих персональных данных (адреса, фамилии, имени, отчества и т.п.).

3.1.3. Сотрудник, предоставивший организации подложные документы или заведомо ложные сведения о себе, несёт **дисциплинарную ответственность** вплоть до **увольнения в соответствии со ст. 81 п. 11 ТК РФ.**

3.2. Права сотрудника.

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

3.2.2. Определять своих представителей для защиты своих персональных данных.

3.2.3. На сохранение и защиту своей личной и семейной тайны.

3.2.4. Обжаловать в судебном порядке любые неправомерные действия организации при обработке и защите персональных данных сотрудника.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКА.

Под обработкой персональных данных сотрудника понимается **получение** (создание), **комбинирование**, **передача, хранение** или любое другое использование персональных данных сотрудника.

4.1. Получение (создание) персональных данных.

Документы, содержащие персональные данные сотрудника, создаются путём:

а) копирования оригиналов (документ об образовании, паспорт, свидетельство ИНН, пенсионное свидетельство СНИЛС);

б) внесения сведений в учётные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, автобиография, медицинское заключение).

Сведения, содержащие персональные данные сотрудника, включаются в его личное дело, карточку формы Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешён лицам, непосредственно использующим персональные данные сотрудника в служебных целях. Перечень должностных лиц определён в пункте 5 настоящего Положения. Указанным должностным лицам **не допускается отвечать** на вопросы, связанные с передачей персональной информации по **телефону или факсу.**

Личное дело после прекращения трудового договора с сотрудником передается в архив, и хранится установленные законодательством сроки.

4. 2. Обязанности организации при обработке персональных данных.

В целях обеспечения законности организация в **соответствии со ст. 86 ТК РФ** при обработке персональных данных сотрудника соблюдает следующие общие требования:

4.2.1. Обработка персональных данных сотрудника осуществляется исключительно в целях содействия сотруднику в обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4.2.2. При определении содержания и объёма обрабатываемых персональных данных сотрудников, организация руководствуется Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

4.2.3. Все персональные данные сотрудника организация получает **у него самого**. Если персональные данные сотрудника, возможно, получить только у третьей стороны, то сотрудник уведомляется об этом заранее и от него получается **письменное согласие,** ему сообщается о целях, характере, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа сотрудника дать письменное согласие на их получение.

4.2.4. Организация не получает и не обрабатывает персональные данные сотрудника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ организация вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

4.2.5. Организация не получает и не обрабатывает персональные данные сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

4.2.6. Защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена организацией за счет её средств (ст. 86 п.7 ТК РФ).

4.2.7. Сотрудники знакомятся под расписку (лист ознакомления) с документами организации, устанавливающими порядок обработки персональных данных сотрудников, а также об их правах и обязанностях в этой области, а именно с Положением о защите персональных данных сотрудников организации (ст. 86 п.8 ТК РФ).

4.2.8. Организация в соответствии с требованиями ст. 88 ТК РФ:

- **не сообщает** персональные данные сотрудника третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом;
- **не сообщает** персональные данные сотрудника в коммерческих целях без его письменного согласия;
- **разрешает доступ** к персональным данным сотрудников только специально уполномоченным лицам, определенным приказом директора организации, при этом указанные лица должны иметь право получать только те персональные

данные сотрудника, которые необходимы для выполнения конкретных функций;

- **не запрашивает** информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции.

4.2.9. **При принятии решений**, затрагивающих интересы сотрудника, организация не основывается на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения (ст. 86 п.6 ТК РФ). Организация **учитывает личные качества сотрудника, его добросовестный и эффективный труд.**

4.3. Хранение персональных данных в отделе по управлению персоналом:

- персональные данные, содержащиеся на бумажных носителях, включённые в состав личных дел, хранятся в запираемом шкафу, установленном в помещении отдела по управлению персоналом. Трудовая книжка, документы воинского учёта, карточка формы Т-2 хранятся в запертом металлическом сейфе.

- персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК руководителя отдела по управлению персоналом. Доступ к ПК руководителя имеет сам руководитель отдела по управлению персоналом.

Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

К обработке, передаче и хранению персональных данных сотрудника имеют доступ сотрудники:

- бухгалтерии;
- сотрудники отдела управления персоналом;

Лица, получающие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности).

5 . ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СОТРУДНИКА.

I. Уполномоченные лица имеют право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц. Все остальные сотрудники имеют право на полную информацию только об их собственных персональных данных и обработке этих данных.

II. Предоставление сведений о персональных данных сотрудников без соответствующего письменного их согласия возможно в следующих случаях:

а) в целях предупреждения угрозы жизни и здоровья сотрудника;

б) при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;

в) при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

Сотрудник, о котором запрашиваются сведения, должен быть уведомлён о передаче его персональных данных третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий, аварий, катастроф.

5.1. Внутренний доступ (доступ внутри организации).

5.1.1. Право доступа к персональным данным сотрудника имеют:

- Директор организации;
- Руководители структурных подразделений, отдела по направлению деятельности (доступ к личным данным только сотрудников своего подразделения, отдела);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам сотрудник, носитель данных.
- сотрудники бухгалтерии;
- сотрудники отдела по управлению персоналом;

5.1.2. Перечень лиц, имеющих доступ к персональным данным сотрудников, определяется приказом директора организации (Приложение к Положению).

5.2. Внешний доступ.

5.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговая инспекция;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

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

5.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным сотрудника только в случае его письменного разрешения.

5.2.4. Другие организации.

- Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с официального письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления сотрудника.
- 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).

Любая передача персональных данных сотрудников происходит только в письменном виде! Запрещена передача данных по телефону, факсу, в электронном виде! Запрос из других организаций должен быть сделан в письменном виде с указанием всех реквизитов лица, запрашивающего информацию, на фирменном бланке.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКА.

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 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.

6.4. «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным являются, как правило, сотрудники, работающие 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.

Для обеспечения внутренней защиты персональных данных сотрудников в организации принят ряд мер:

- утверждён состав сотрудников, имеющих доступ к персональным данным;
- установлено строгое избирательное и обоснованное распределение документов и информации между сотрудниками, которое внесено в должностные инструкции;
- рабочее пространство помещения отдела сформировано так, чтобы исключить бесконтрольное использование защищаемой информации;
- после утверждения настоящего Положения будет установлен контроль за знанием и выполнением сотрудниками отдела по управлению персонала

требований настоящего Положения с целью предупреждения утраты ценных сведений при работе с конфиденциальными, персональными документами. Контроль будет возложен на руководителя отдела с занесением данной функции в должностную инструкцию;

- установлен в помещении отдела по управлению персоналом металлический сейф, для хранения трудовых книжек, шкаф с замком и два ящика стола, запираемые на ключ;
- установлен пароль на ПК руководителя отдела по управлению персоналом, в котором храниться база персональных данных сотрудников МБДОУ д/с №3 «Звездочка»
- копия базы персональных данных записана на флэш-карту, которая хранится в металлическом сейфе, в помещении отдела по управлению персоналом;
- введён **запрет** сотрудникам отдела по управлению персоналом выдавать **личные дела на рабочие места** руководителей отделов и подразделений. Личные дела могут выдаваться на рабочие места только директору, сотрудникам отдела по управлению персоналом и в исключительных случаях, по письменному разрешению директора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации сотрудника). Все остальные сотрудники, имеющие доступ к персональным данным, могут изучать личные дела или иные документы **только в помещении отдела** по управлению персоналом в присутствии одного из сотрудников этого отдела.

6.5. «Внешняя защита».

6.5.1**.** Для защиты персональных данных, находящихся в ПК руководителя отдела по управлению персоналом системным администратором организации созданы целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, которое возможно захочет совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к базе персональных данных 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 организации. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе по управлению персоналом.

6.5.2. Все лица, связанные с получением, обработкой и защитой персональных данных, подписывают **обязательство о неразглашении персональных** данных сотрудников и **лист ознакомления** с настоящим Положением о персонале.

При приёме на работу нового сотрудника, перед заключением трудового договора в соответствии со ст. 68 ТК РФ, организация в лице одного из сотрудников отдела по управлению персоналом знакомит нового сотрудника под роспись с Положением о защите персональных данных (лист ознакомления). При приёме на работу нового сотрудника, в служебные обязанности которого входит работа с персональными данными (перечень лиц в Приложении «Приказ»), перед заключением трудового договора, новый сотрудник подписывает обязательство о неразглашении персональных данных и лист ознакомления с Положением о защите персональных данных под роспись.

6.5.3. По возможности персональные данные сотрудников обезличиваются.

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 организации, получающий для работы конфиденциальный документ и внесённый в перечень лиц имеющих доступ к персональной информации, несет единоличную ответственность **за сохранность носителя** (бумажного и электронного) и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами (ст. 90 ТК РФ).

7.6. За неисполнение или ненадлежащее исполнение сотрудником возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера, за нарушение норм, регулирующих получение, обработку, хранение и защиту персональных данных сотрудника организация применяет следующие предусмотренные Трудовым Кодексом дисциплинарные взыскания:

а) замечание;

б) выговор;

в) предупреждение о неполном должностном соответствии;

г) освобождение от занимаемой должности с переводом;

д) **увольнение ст. 81 п. 6 (в) ТК РФ.**

По факту нарушения норм настоящего Положения о защите персональных данных, в организации проводится **служебное расследование**. Служебное расследование проводится в минимально короткий срок, но не более одного месяца со дня обнаружения указанного факта. Перед решением применить меры соответствующего взыскания сотрудник предоставляет организации **письменное объяснение.** Если по истечении двух рабочих дней указанное объяснение не предоставлено, то составляется соответствующий акт о нарушении норм Положения о защите персональных данных. **Приказ** заведующего о применении взыскания объявляется сотруднику под личную роспись не позднее трёх рабочих дней со дня издания приказа. При отказе сотрудника от ознакомления с приказом директора составляется акт (ст. 193 ТК РФ). Непредставление сотрудником объяснения не является препятствием для применения дисциплинарного взыскания (ст. 193 п. 2 ТК РФ). В трудовой книжке при **увольнении** сотрудника вносится запись: «Трудовой договор расторгнут по инициативе работодателя ввиду разглашения персональных данных другого работника, ставших известными сотруднику в связи с исполнением трудовых обязанностей, подпункт «в» пункта 6 81 Трудового кодекса Российской Федерации».

За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание. Если в течение года со дня применения дисциплинарного взыскания сотрудник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Организация до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с сотрудника по собственной инициативе, по письменному заявлению сотрудника или по ходатайству его непосредственного руководителя.

7.7. Сотрудники отдела по управлению персоналом, в обязанность которых входит ведение персональных данных сотрудников, 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.

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

7.9. 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.

7.10. Неправомерность организации по сбору и использованию персональных данных может быть установлена только в судебном порядке

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

8.1. Настоящее Положение вступает в силу с момента его утверждения директором и вводится в действие его приказом.

8.2. Настоящее Положение **обязательно для всех** сотрудников организации.

Согласовано:

Делопроизводитель
Литвинова Я.В.