

ПРИНЯТО на Общем
собрании работников
Протокол № 2
от 16 марта 2015 года

УТВЕРЖДЕНО
Приказом заведующего МДОУ
№ 80 «Гномик»
Приказ № 26/Л
от 16 марта 2015 года

ПОЛОЖЕНИЕ
о защите персональных данных
Муниципального дошкольного образовательного учреждения
«Детский сад комбинированного вида № 80 «Гномик»

I. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, принятым Федеральным законом № 197-ФЗ от 30.12.2001 г., Федеральным законом Российской Федерации "Об информации, информационных технологиях и о защите информации" № 149-ФЗ от 27.07.2006 г., Федеральным законом Российской Федерации "О персональных данных" № 152-ФЗ от 27.07.2006 г., Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г. и другими нормативными правовыми актами.

1.2. Настоящее Положение определяет порядок обработки персональных данных в Муниципальном дошкольном образовательном учреждении «Детский сад комбинированного вида № 80 «Гномик» (Далее - Учреждение) и гарантии конфиденциальности сведений, предоставляемых гражданами в Учреждение.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в настоящее Положение вносятся приказом руководителя Учреждения.

1.4. Все работники Учреждения должны быть ознакомлены с настоящим Положением под подпись.

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

II. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

– персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место

рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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

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

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

– использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении граждан 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, в том числе их передачи;

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

– обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному гражданину;

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

2.2. В состав персональных данных граждан входят:

- фамилия, имя, отчество;
- дата рождения;

- паспортные данные;
- место рождения;
- гражданство;
- образование (оконченные учебные заведения и год окончания, специальности (направления) и квалификации, наличие ученых степеней);
- сведения о составе семьи;
- сведения о периодах трудовой деятельности;
- отношение к воинской обязанности и воинское звание;
- место регистрации и место фактического проживания,
- номер страхового свидетельства обязательного пенсионного страхования;
- идентификационный номер налогоплательщика;
- номер полиса обязательного медицинского страхования;
- выполняемая работа, занимаемая должность, дата назначения, переводы на иные должности и основания назначения (перевода);
- номер домашнего и мобильного телефона;
- номер служебного телефона;
- условия и размер оплаты труда;
- решения соответствующих конкурсных комиссий;
- прохождение аттестаций, даты прохождения и принятые аттестационными комиссиями решения и вынесенные рекомендации;
- проведение служебных проверок и наложение дисциплинарных взысканий;
- награждение государственными и ведомственными наградами, иными наградами;
- пребывание в отпусках и направлении в командировки;
- реквизиты расчетного (текущего) счета.

III. Обработка персональных данных

3.1. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в

отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных, либо были извлечены из нее.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ

3.2. Учреждение не имеет права получать и обрабатывать персональные данные граждан об их политических, религиозных и иных убеждениях и частной жизни, состоянии здоровья без письменного согласия субъекта персональных данных. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Учреждение вправе получать и обрабатывать данные о частной жизни гражданина только с его письменного согласия.

Учреждение не имеет права получать и обрабатывать персональные данные граждан об их членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

При принятии решений, затрагивающих интересы граждан, Учреждение не имеет права основываться на персональных данных граждан, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.3. На основании норм Трудового кодекса РФ (ст. 86), а также исходя из положений п.2 ст.6 ФЗ РФ "О персональных данных", обработка персональных данных осуществляется Учреждением без письменного согласия гражданина, за исключением случаев, предусмотренных федеральным законом.

Также, обработка персональных данных осуществляется Учреждением без письменного согласия граждан в случаях обработки персональных данных осуществляемых в целях исполнения договора, одной из сторон которого является субъект персональных данных, для статистических или иных научных целей при условии обязательного обезличивания персональных данных, для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

Примечание: В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные

книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

IV. Получение персональных данных

4.1. Все персональные данные о гражданине Учреждение может получить у него самого.

4.2. Граждане предоставляют в Учреждение достоверные сведения о себе и своевременно сообщают ему об изменении своих персональных данных. Учреждение проверяет достоверность сведений, предоставленных гражданами, сверяя данные, предоставленные гражданами, с имеющимися в Учреждении документами.

4.3. В случаях, когда Учреждение может получить необходимые персональные данные граждан только у третьего лица, Учреждение должно уведомить об этом гражданина и получить от него письменное согласие по установленной форме.

Учреждение обязано сообщить гражданину о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа гражданину дать письменное согласие на их получение.

V. Хранение персональных данных

5.1. Персональные данные граждан хранятся в информационных системах персональных данных.

Персональные данные хранятся как в электронном виде, так и на бумажных носителях. Доступ к электронным базам данных, содержащим персональные данные, обеспечиваются системой защиты персональных данных.

При обработке персональных данных, осуществляемой без использования средств автоматизации, хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях, должно обеспечиваться раздельное хранение.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

5.2. Сотрудник Учреждения, имеющий доступ к персональным данным граждан в связи с исполнением трудовых обязанностей:

обеспечивает хранение информации, содержащей персональные данные, исключая доступ к ним третьих лиц.

В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные, а также сотрудник обязан исключить несанкционированный доступ к техническим средствам обработки персональных данных.

При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные лицу, на которое локальным актом Учреждения (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

Примечание: В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию руководителя структурного подразделения либо руководителя Учреждения.

При увольнении сотрудника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные граждан, передаются другому сотруднику, имеющему доступ к персональным данным по указанию руководителя структурного подразделения либо руководителя Учреждения.

VI. Использование (доступ, передача, комбинирование и т.д.) персональных данных

6.1. Доступ к персональным данным имеют сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией руководителя Учреждения, доступ к персональным данным может быть предоставлен иному работнику, должность которого не включена в Перечень должностей сотрудников, имеющих доступ к персональным данным, и которым они необходимы в связи с исполнением трудовых обязанностей.

6.2. В случае если Учреждение 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 в Учреждение, то соответствующие данные предоставляются Учреждением 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.

6.3. Процедура оформления доступа к персональным данным включает в себя:

-ознакомление работника под подпись с настоящим Положением.

Примечание: При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных, с данными актами также производится ознакомление работника под подпись.

-истребование с сотрудника (за исключением руководителя Учреждения) письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки, подготовленного по установленной форме.

6.4. Сотрудники Учреждения, имеющие доступ к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения конкретных трудовых функций.

6.5. Доступ к персональным данным без специального разрешения имеют работники, занимающие в организации следующие должности:

-руководитель Учреждения;

-исполняющий обязанности руководителя Учреждения.

6.6. Допуск к персональным данным других сотрудников Учреждения, не имеющих надлежащим образом оформленного доступа, запрещается.

6.7. Гражданин имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Гражданин имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

6.8. Запрещено передавать персональные данные субъекта персональных данных третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом. При передаче необходимо руководствоваться договором с третьим лицом (организацией), существенным условием которого должна быть обязанность обеспечения указанным лицом (организацией) конфиденциальности и безопасности персональных данных при их обработке. При предоставлении персональных данных третьим лицам фиксировать факт передачи, подкрепленный подписью принимающего лица.

Запрещено передавать персональные данные по телефону, факсу, на основании устных запросов.

При передаче персональных данных по каналам связи, сетям общего пользования (Интернет) использовать криптографические средства защиты информации.

Учреждение вправе передавать персональные данные граждан в структурные подразделения только на основании представленного письменного запроса (приказа) с указанием цели сбора данных сведений, в случае необходимости исполнения сотрудниками соответствующих структурных подразделений своих трудовых обязанностей.

При передаче персональных данных граждан, сотрудники Учреждения предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство в соответствии с п. 3.11. настоящего Положения.

6.9. Передача (обмен и т.д.) персональных данных между подразделениями Учреждения осуществляется только между сотрудниками, имеющими доступ к персональным данным.

VII. Доступ к персональным данным третьих лиц (физических и юридических)

7.2. Передача персональных данных третьим лицам осуществляется только с письменного согласия гражданина, которое оформляется по установленной форме и должно включать в себя:

- фамилию, имя, отчество, адрес гражданина, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес юридического лица, получающего согласие гражданина;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие гражданин;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Примечание: Согласия граждан на передачу их персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина; когда третьи лица оказывают услуги работодателю на основании заключенных договоров, а также в случаях, установленных федеральным законом и настоящим Положением.

7.3. Не допускается передача персональных данных граждан в коммерческих целях без его письменного согласия.

7.4. Сотрудники Учреждения, передающие персональные данные граждан третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные граждан. Акт должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

-предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

Передача документов (иных материальных носителей), содержащих персональные данные, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Учреждением;
- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных гражданина;
- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных несет сотрудник, а также руководитель структурного подразделения, осуществляющего передачу персональных данных третьим лицам.

7.5. Представителю граждан (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя гражданина;
- письменного заявления гражданина, написанного в присутствии сотрудника Учреждения (если заявление написано не в присутствии сотрудника Учреждения, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в архиве Учреждения.

7.6. Предоставление персональных данных государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.

7.7. Персональные данные могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого гражданина, за исключением случаев, когда передача персональных данных без его согласия допускается действующим законодательством РФ.

7.8. Документы, содержащие персональные данные, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с

сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

VIII. Организация защиты персональных данных

8.1. 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.

8.2. 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.

8.3. 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.

8.4. Защита персональных данных от неправомерного их использования или утраты обеспечивается Учреждением за счет средств Учреждения в порядке, установленном федеральными законами.

8.5. Защите подлежат:

- информация о персональных данных;
- документы, содержащие персональные данные;
- персональные данные, содержащиеся на электронных носителях.

IX. Внутренняя защита

9.1. 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 Учреждения.

9.2. Для обеспечения внутренней защиты персональных данных 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;
- 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;
- личные дела могут выдаваться только заведующему или заместителю заведующего по воспитательной и методической работе (например, при подготовке материалов для аттестации сотрудника).

9.3. Защита сведений, хранящихся в электронных базах данных Учреждения, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается системой защиты персональных данных.

Х. Внешняя защита

10.1. Для защиты персональных данных 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.

10.2. 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 в кадровой работе.

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

- порядок приема, учета и контроля деятельности посетителей;

- пропускной режим Учреждения;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и беседах.

10.4. По возможности персональные данные обезличиваются.

10.5. Кроме мер защиты персональных данных, установленных законодательством, Учреждение, сотрудники и их представители могут вырабатывать совместные меры защиты персональных данных.

XI. Заключительные положения

11.1. Иные права, обязанности, действия сотрудников, в трудовые обязанности которых входит обработка персональных данных, определяются также должностными инструкциями.

11.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

11.3. Разглашение персональных данных в Учреждении (передача их посторонним лицам, в том числе, работникам Учреждения, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Учреждения, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

Сотрудник Учреждения, имеющий доступ к персональным данным и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению (п.7 ст. 243 Трудового кодекса РФ).

11.4. Сотрудники Учреждения, имеющие доступ к персональным данным, виновные в незаконном разглашении или использовании персональных данных работодателя без согласия граждан из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.