

Согласованы

Протокол № 30 от 15.01.2014г.

Председатель первичной организации
МКДОУ д/с комбинированного вида
№ 10

С.Н. Григорьева

Утверждены

Приказ № 4/3-д от 20.01.2014г.

Заведующий МКДОУ д/с
комбинированного вида № 10

З.И. Брыли



**Изменения к положению
об обеспечении безопасности персональных данных при их обработке
в информационной системе
муниципального казённого дошкольного образовательного учреждения
детского сада комбинированного вида № 10
(МКДОУ д/с комбинированного вида № 10)**

1. Пункт 1. Общие положения, изложить в следующей редакции:

Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных», уставом МКДОУ д/с комбинированного вида № 10 и определяет порядок обработки и защиты персональных данных работников МКДОУ д/с комбинированного вида № 10 (далее по тексту МКДОУ), воспитанников и их родителей (законных представителей).

2. Пункт 1, подпункт 1.3. изложить в следующей редакции:

- документы, предъявляемые при заключении договора между родителем (законным представителем) и МКДОУ (паспорт или документ, удостоверяющий личность; страховое свидетельство государственного пенсионного страхования; ИНН; данные о регистрации и месте работы).

Перечень персональных данных воспитанников и их родителей (законных представителей) представлен в приложении 2.

3. Пункт 2. изложить в следующей редакции:

К основным принципам обработки персональных данных можно отнести:

- а) принцип законности целей и способов обработки персональных данных;
- б) принцип соответствия объема и характера обрабатываемых персональных данных, способов их обработки и целям обработки персональных данных;
- в) принцип достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к заявленным при их сборе целям;
- г) принцип недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- д) принцип защиты персональных данных от неправомерного доступа и их использования или утраты.

При обработке персональных данных должны соблюдаться, согласно положениям, статьи 86 Трудового кодекса РФ, следующие общие требования:

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;

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

3) все 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 и последствиях отказа работника дать письменное согласие на их получение;

4) 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, в соответствии со статьей 24

Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) при принятии решений, затрагивающих интересы работника, работодатель не имеет право основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

6) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ или иными федеральными законами;

7) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работником, а также об их правах и обязанностях в этой области;

8) работники не должны отказываться от своих прав на сохранение и защиту тайны;

9) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

4. Пункт 4. изложить в следующей редакции:

Документы, содержащие информацию о персональных данных работников, воспитанников и их родителей (законных представителей) хранятся на бумажном и электронном носителе в расчетном и экономическом отделах централизованной бухгалтерии. Доступ к такой информации без получения специального разрешения имеют главный бухгалтер, сотрудники управления бухгалтерского учета и финансового контроля. Иные сотрудники МКДОУ не могут иметь доступ к персональным данным работников. Со сторонними работниками, сопровождающими работу информационных систем, следует заключать договора о неразглашении персональных данных работников и воспитанников.

Пункт 5. изложить в следующей редакции:

Согласно положения «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» от 17 ноября 2007г. №781 . под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Работа по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений (с помощью систем сигнализации), в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения в эти помещения посторонних лиц.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

с) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

Контроль за организацией доступа к персональным данным работников, воспитанников и их родителей (законных представителей) МКДОУ возложить на делопроизводителя.

5. Пункт 8. изложить в следующей редакции:

Обязанности работников МКДОУ по обеспечению достоверности его персональных данных.

Работники и родители (законные представители) воспитанников должны быть заранее предупреждены о необходимости предоставления достоверных сведений и о возможности ответственности в случае нарушения своей обязанности.

Правовой основой для установления обязанности работников и родителей (законных представителей) по предоставлению достоверной информации о своих персональных данных служит положение статьи 8 ТК РФ, устанавливающей полномочия работодателя по принятию локальных нормативных актов, содержащих нормы трудового права.

6. Пункт 10. изложить в следующей редакции:

Сотрудники МКДОУ ответственные за работу с персональными данными, должны четко знать случаи, при которых они могут передать информацию о работнике и воспитаннике запрашивающим лицам. К таким случаям, как правило, относят запросы о

получении информации о работниках и воспитанниках, направленные различными государственными органами.

Наиболее вероятно, что подобные запросы поступают из судебных или правоохранительных органов.

На основании части 2 статьи 57 Гражданского процессуального кодекса Российской Федерации (ГПК РФ) суд вправе выдать работнику запрос для получения доказательства или направить запрос самостоятельно:

Статья 57. Представление и истребование доказательств

1. Доказательства представляются сторонами и другими лицами, участвующими в деле. Суд вправе предложить им представить дополнительные доказательства. В случае, если представление необходимых доказательств для этих лиц затруднительно, суд по их ходатайству оказывает содействие в собирании и истребовании доказательств.

2. В ходатайстве об истребовании доказательства должно быть обозначено доказательство, а также указано, какие обстоятельства, имеющие значение для правильного рассмотрения и разрешения дела, могут быть подтверждены или опровергнуты этим доказательством, указаны причины, препятствующие получению доказательства, и место нахождения доказательства. Суд выдает стороне запрос для получения доказательства или запрашивает доказательство непосредственно. Лицо, у которого находится истребуемое судом доказательство, направляет его в суд или передает на руки лицу, имеющему соответствующий запрос, для представления в суд.

3. Должностные лица или граждане, не имеющие возможности представить истребуемое доказательство вообще или в установленный судом срок, должны известить об этом суд в течение пяти дней со дня получения запроса с указанием причин. В случае неисполнения суда, а также в случае невыполнения требования суда о представлении доказательства по причинам, признанным судом неуважительными, на виновных должностных лиц или на граждан, не являющихся лицами, участвующими в деле, налагается штраф - на должностных лиц в размере до десяти установленных федеральным законом минимальных размеров оплаты труда, на граждан - до пяти установленных федеральным законом минимальных размеров оплаты труда.

4. Наложение штрафа не освобождает соответствующих должностных лиц и граждан, владеющих истребуемым доказательством, от обязанности представления его суду.

При этом следует учитывать то обстоятельство, что виновным должностным лицом (вне зависимости от того, на кого возложены в университете обязанности по работе со сведениями, составляющими персональные данные) будет признан ректор университета, поэтому, несмотря на незначительный размер штрафа, судебный запрос должен быть исполнен в срок и в полном объеме.

В ситуациях, когда предоставление сведений о персональных данных работника и студента может потребоваться при ведении расследования по уголовным делам. Статья 21 Уголовно-процессуального кодекса Российской Федерации (УПК РФ) предусмотрено, что запросы прокурора, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий, установленных УПК РФ, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами.

Статья 21. Обязанность осуществления уголовного преследования

1. Уголовное преследование от имени государства по уголовным делам публичного и частного-публичного обвинения осуществляют прокурор, а также следователь и дознаватель.

2. В каждом случае обнаружения признаков преступления прокурор, следователь, орган дознания и дознаватель принимают предусмотренные настоящим Кодексом меры по установлению события преступления, изобличению лица или лиц, виновных в совершении преступления.

3. Следователь, а также с согласия прокурора дознаватель в случаях, предусмотренных частью четвертой статьи 20 настоящего Кодекса, уполномочены осуществлять уголовное преследование по уголовным делам независимо от волеизъявления потерпевшего.

4. Требования, поручения и запросы прокурора, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий, установленных настоящим Кодексом, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами.

7. Пункт 11. изложить в следующей редакции:

Ответственность за нарушение законодательства об охране персональных данных может быть дисциплинарной, административной и уголовной.

К дисциплинарной ответственности может быть привлечен работник управления кадров, бухгалтерии, иного подразделения, использующего в своей работе персональные данные.

В подпункте «в» пункта 6 статьи 81 Трудового кодекса РФ предусматривается, что «разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника».

К административной ответственности могут быть привлечены как работники управления кадров и иных подразделений, так и заведующий МКДОУ, так и организация в целом на основании статей 2.4. КоАП РФ и 13.11. КоАП РФ.

Статья 2.4 КОАП (кодекса об административных правонарушениях) РФ Административная ответственность должностных лиц.

Административной ответственности подлежит должностное лицо в случае совершения им административного правонарушения в связи с неисполнением либо ненадлежащим исполнением своих служебных обязанностей.

Примечание. Под должностным лицом в настоящем Кодексе следует понимать лицо, постоянно, временно или в соответствии со специальными полномочиями осуществляющее функции представителя власти, то есть наделенное в установленном законом порядке распорядительными полномочиями в отношении лиц, не находящихся в служебной зависимости от него, а равно лицо, выполняющее организационно-распорядительные или административно-хозяйственные функции в государственных органах, органах местного самоуправления, государственных и муниципальных организациях, а также в Вооруженных Силах Российской Федерации, других войсках и воинских формированиях Российской Федерации. Совершившие административные правонарушения в связи с выполнением организационно-распорядительных или административно-хозяйственных функций руководители и другие работники иных организаций, а также лица, осуществляющие предпринимательскую деятельность без образования юридического лица, несут административную ответственность как должностные лица, если законом не установлено иное.

Статья 13.11 КОАП (кодекса об административных правонарушениях) РФ. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

Уголовная ответственность за нарушение неприкосновенности частной жизни предусмотрена статьей 137 УК РФ. В качестве наказания за это преступление предусмотрено наложение штрафа в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательные работы на срок от ста двадцати до ста восьмидесяти часов, либо исправительные работы на срок до одного года, либо арест на срок до четырех месяцев.

Если же преступление совершено с использованием служебного положения, то наказанием может быть штраф в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, лишение права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арест на срок от четырех до шести месяцев (часть 2 статьи 137 УК РФ).

Приказ № 4/3-д

От 20.01.2014г

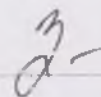
по МКДОУ д/с комбинированного вида № 10

“О внесении изменений в приказ от 19.01.2011 № 2-д «Об организации работ по защите информации, содержащие персональные данные»”

В связи с расторжением трудового договора с делопроизводителем Дятловой Н.И. и на основании назначения на должность делопроизводителя Богомазовой Е.А., приказываю:

1. Считать утратившим силу приказ от 27.08.2012 № 35-д «О внесении изменений в приказ от 19.01.2011 № 2-д «Об организации работ по защите информации, содержащие персональные данные».
2. Внести в приказ от 19.01.2011 № 2-д «Об организации работ по защите информации, содержащие персональные данные» следующие изменения:
 - 2.1. Пункт 3 приказа изложить в следующей редакции:
«3. Назначить ответственным за защиту информации, содержащей персональные данные работников МКДОУ д/с комбинированного вида № 10 и родителей (законных представителей) воспитанников, посещающих МКДОУ д/с комбинированного вида № 10 делопроизводителя Богомазову Е.А.»
 - 2.2. Пункт 5 приказа изложить в следующей редакции:
«4. Назначить ответственным за защиту информации, содержащей персональные данные педагогических работников МКДОУ д/с комбинированного вида № 10 заместителя заведующего по воспитательной и методической работе Потапову Е.В.»
 - 2.3. Пункт 9 приказа изложить в следующей редакции:
«9. Назначить ответственным за обеспечение безопасности персональных данных МКДОУ д/с комбинированного вида № 10 делопроизводителя Богомазову Е.А.»
 - 2.4. Пункт 10 приказа изложить в следующей редакции:
«10. Назначить ответственных за эксплуатацию объектов ВТ:
 - Потапову Е.В., заместителя заведующего по воспитательной и методической работе;
 - Богомазову Е.А., делопроизводителя.»
3. Утвердить изменения к Перечню лиц, допущенным к персональным данным работников, воспитанников и их родителей (законных представителей) в МКДОУ д/с комбинированного вида № 10.
4. Утвердить изменения к Положению об обеспечении безопасности персональных данных при обработке в информационной системе МКДОУ д/с комбинированного вида № 10.
5. Данные изменения вступают в силу 13.01.2014г.

Заведующий МКДОУ д/с комбинированного вида № 10

 /З.И.Брыль/

С приказом ознакомлены:

