УТВЕРЖДЕНА
приказом МКДОУ «Детский сад
№34 «Радуга»
от 03.07.2017г. №111-Т

ИНСТРУКЦИЯ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Работники Муниципального казенного дошкольного образовательного учреждения «Детский сад №34 «Радуга» (далее – Организация), уполномоченные на обработку персональных данных, а так же работники, работающие в помещениях, в которых ведётся обработка персональных данных, должны быть ознакомлены с данной инструкцией.

1.2. Работники, допущенные к обработке персональных данных, обязаны строго соблюдать установленные правила работы и несут персональную ответственность за обеспечение безопасности информации.

II. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации.

2.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании Перечня должностей Муниципального казенного дошкольного образовательного учреждения «Детский сад №34 «Радуга», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

2.3. Должна быть обеспечена сохранность носителей персональных данных и средств защиты информации, а также исключена возможность неконтролируемого пребывания посторонних лиц в помещениях, в которых ведется обработка персональных данных.

2.4. Компьютеры и (или) электронные папки (каталоги), в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены

индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

2.5. Осуществлять обработку и хранение персональных данных, не внесённых в Перечень персональных данных, обрабатываемых в Организации, запрещается.

2.6. Работникам Организации, работающим с персональными данными, запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении.

2.7. Работникам Организации, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем Организации формирование и хранение баз данных (списков, картотек, файловых архивов и др.), содержащих персональные данные, запрещается.

2.8. Передача персональных данных допускается только в случаях, установленных действующим законодательством Российской Федерации, инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

2.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан.

2.10. Все компоненты программного и аппаратного обеспечения информационной системы персональных данных должны использоваться работниками Организации только в служебных целях. Использование их в других целях запрещается.

2.11. Запрещается приём посетителей в помещениях, во время осуществления обработки персональных данных, кроме случаев, возникающих при необходимости обработки персональных данных самого посетителя.

2.12. Пользователю запрещается самовольно изменять конфигурацию аппаратно-программных средств информационной системы или устанавливать дополнительно любые программные и аппаратные средства. Исключением являются только те случаи, когда пользователь, при непосредственном исполнении своих должностных обязанностей, реализует назначенные приказом права администратора (супервизора) этой информационной системы. Кроме того, все изменения конфигурации технических и программных средств

осуществляются только с участием администратора безопасности информационной системы персональных данных.

2.13. Категорически запрещается записывать и хранить персональные данные на неучтённых носителях, а также использовать носители с выявленными неисправностями.

2.14. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе в информационно-телекоммуникационной сети Интернет, запрещается.

2.15. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) или съёмных маркированных носителей;

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

- постоянное использование антивирусного обеспечения для обнаружения заражённых файлов;

- незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

2.16. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

III. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, в том числе (под личную подпись) с данной инструкцией.

3.2. Необходимо обеспечить раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своём согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.4. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путём обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путём фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путём изготовления нового материального носителя с уточнёнными персональными данными.

IV. ПОРЯДОК УЧЁТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЁМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЁРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИЯ

4.1. Все находящиеся на хранении и в обращении съёмные носители с персональными данными подлежат учёту. Каждый съёмный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учётный номер.

4.2. Учтённый съёмный носитель получают для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале учета носителей персональных данных. По окончании работ пользователь сдаёт съёмный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета носителей персональных данных.

4.3. Запрещается:

- хранить съёмные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съёмные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

4.4. При отправке или передаче персональных данных адресатам на съёмные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съёмных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.5. О фактах утраты съёмных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель Организации. На утраченные носители составляется акт. Соответствующие отметки вносятся в Журнал учета носителей персональных данных.

4.6. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат передаче администратору безопасности для уничтожения.

V. ОБЯЗАННОСТИ РАБОТНИКОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В обязанности работников Организации входит:

5.1.1. Своевременный и точный ввод данных в информационную систему персональных данных.

5.1.2. Немедленно ставить в известность администратора безопасности о случаях обнаружения непредусмотренных отводов кабелей и проводов, изменений алгоритмов функционирования технических и программных средств автоматизированного рабочего места, нарушениях нормальной работы средств защиты, которые свидетельствуют о возможных попытках или фактах несанкционированного доступа к информации.

5.1.3. По окончании рабочего дня сдача полученных во временное пользование съёмных носителей (гибких магнитных дисков, flash-носителей), а так же, при необходимости, индивидуальных идентификаторов, которые должны быть помещены в сейф или в металлический шкаф.

5.1.4. После окончания обработки персональных данных и изъятия съёмных накопителей информации необходимо выключить электропитание автоматизированного рабочего места.

VI. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ

6.1. Работник несёт ответственность за содержание вводимой им информации.

6.2. Работник (пользователь информационной системы персональных данных) несёт ответственность за сохранность и правильное использование получаемых в ходе выполнения работ машинных носителей и машинных документов с персональными данными. Степень конфиденциальности съемных носителей информации и документов, получаемых в ходе автоматизированной обработки информации, определяется администратором безопасности.

6.3. Работники, осуществляющие обработку или хранение персональных данных, несут ответственность за обеспечение их информационной безопасности.

6.4. Лица, виновные в нарушении норм, регулирующих обработку и хранение персональных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации, в том числе за:

6.4.1. Разглашение конфиденциальной информации (персональных данных) в процессе осуществления своей деятельности в пределах, определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.

6.4.2. Причинение материального ущерба в пределах, определённых действующим трудовым, уголовным и гражданским законодательством Российской Федерации.