Приложение № 3
к приказу №72-од от 05.04.16

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТА ИЛИ КОНТРАГЕНТА
В МБОУ Школе №77 г.о. Самара

1. Общие положения

1.1. Целью данного Положения является защита персональных данных Клиентов или Контрагентов от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации»

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом Директора МБОУ Школы № 77 г.о. Самара и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным клиентов.

2. Понятие и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

Оператор - МБОУ Школа № 77 г.о. Самара, вступившее в договорные отношения с клиентом/(контрагентом) или оказывающее услуги юридическому лицу и индивидуальному предпринимателю.

Клиент– физическое лицо, потребитель услуг, субъект персональных данных

Контрагент – физическое лицо, представитель – физическое лицо юридического лица и индивидуального предпринимателя, субъект персональных данных, вступившие с МБОУ Школой № 77 г.о. Самара в договорные отношения.

Персональные данные клиента/(контрагента)– информация, необходимая исполнителю в связи с договорными отношениями и касающиеся конкретного клиента/(контрагента) Под информацией о клиента/(контрагента) понимаются сведения о фактах, событиях и обстоятельствах жизни клиента/(контрагента) позволяющие идентифицировать его личность.

2.2. В состав персональных данных клиента/(контрагента) входят:

- фамилия, имя, отчество заявителя;
- адрес проживания и адрес регистрации;
- телефон;
- паспортные данные;
- место работы;
- фамилия, имя, отчество ребенка;
- свидетельство о рождении ребенка (паспортные данные обучающихся 9-11 классов);
- место проживания и место регистрации ребенка.

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

3. Обработка персональных данных

3.1. Под обработкой персональных данных клиента/(контрагента) понимается сбор, систематизация, накопление, хранение, уточнение, использование, обезличивание, блокирование, уничтожение или любое другое использование персональных данных клиента/(контрагента).

3.2. В целях обеспечения прав и свобод человека и гражданина исполнитель и его представители при обработке персональных данных клиента/(контрагента) обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных клиента/(контрагента) может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством РФ.

3.2.2. При определении объема и содержания, обрабатываемых персональных данных клиента/(контрагента) исполнитель должен руководствоваться Конституцией Российской Федерации, и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим клиентом/(контрагент), так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у него самого. Если персональные данные клиента/(контрагента) возможно, получить только у третьей стороны, то клиент/(контрагент) должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Исполнитель должен сообщить клиенту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа клиента/(контрагента) дать письменное согласие на их получение.

3.2.5. Исполнитель не имеет права получать и обрабатывать персональные данные клиента/(контрагента) о его политических, религиозных и иных убеждениях и частной жизни.

3.2.6. Исполнитель не имеет право получать и обрабатывать персональные данные клиента/(контрагента) о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных клиента/(контрагента) могут иметь доступ сотрудники:

директор МБОУ Школы № 77 г.о. Самара, зам.директора по УВР, зам.директора по ВР, методист АСУ РСО, ответственный по безопасности ПД, главный бухгалтер, бухгалтер, секретарь, классные руководители, зам.директора по питанию, зам.директора по безопасности, заведующий библиотекой, учителя-предметники.

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

3.4.1. 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.

3.5. Передача персональных данных клиента/(контрагента) возможна только с согласия клиента/(контрагента) или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных клиента/(контрагента) исполнитель должен соблюдать следующие требования:

- не сообщать персональные данные клиента/(контрагента) третьей стороне без письменного согласия клиента/(контрагента), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью клиента/(контрагента), а также в случаях, установленных федеральным законом;

- не сообщать персональные данные клиента/(контрагента) в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные клиента/(контрагента), 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 клиента/(контрагента), обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными клиентов, порядке, установленном федеральными законами;

- разрешать доступ к персональным данным клиента/(контрагента) только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные клиента/(контрагента), которые необходимы для выполнения конкретных функций;

- передавать персональные данные клиента/(контрагента) представителям клиента/(контрагента) в порядке, установленном договорным соглашением, и ограничивать эту информацию только теми персональными данными клиента/(контрагента), которые необходимы для выполнения указанными представителями их функций.

3.5.2. 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.

3.5.3. При передаче персональных данных клиента/(контрагента), потребителям (в том числе и в коммерческих целях), за пределы организации, исполнитель не должен сообщать эти данные третьей стороне без письменного согласия клиента/(контрагента), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью клиента/(контрагента) или в случаях, установленных федеральным законом.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиента/(контрагента) распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

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

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным клиента/(контрагента) имеют:

директор МБОУ Школы № 77 г.о. Самара, зам.директора по УВР, зам.директора по ВР, методист АСУ РСО, ответственный по безопасности ПД, главный бухгалтер, бухгалтер, секретарь, классные руководители, зам.директора по питанию, зам.директора по безопасности, заведующий библиотекой, учителя-предметники.

4.1.2. Перечень лиц, имеющих доступ к персональным данным клиента/(контрагента), определяется приказом Директора МБОУ Школы №77 г.о. Самара организации.

4.2. Внешний доступ.

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

- налоговые инспекции;

- правоохранительные органы;

- органы статистики;

- страховые агентства;

- военкоматы;

- органы социального страхования;

- пенсионные фонды;

- подразделения муниципальных органов управления;

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

4.2.3. Персональные данные клиента/(контрагента) могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого клиента/(контрагента).

5. Защита персональных данных

5.1. 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.

5.2. 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.

5.3. 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.

5.4. Защита персональных данных клиента/(контрагента) от неправомерного их использования или утраты должна быть обеспечена исполнителем за счет его средств, в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. 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 организации.

5.5.2. Для обеспечения внутренней защиты персональных данных клиентов/(контрагентов) 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;

- 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 работников подразделения;

- воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

5.5.3. Защита персональных данных клиента/(контрагента) на электронных носителях.

Все папки, содержащие персональные данные клиента/(контрагента), должны быть защищены паролем, который сообщается руководителю службы управления персоналом и руководителю службы информационных технологий.

Доступ к автоматизированным рабочим местам/, содержащие персональные данные

Осуществляется исключительно по сертификату электронной подписи ответственного лица.

5.6. «Внешняя защита».

5.6.1. Для защиты конфиденциальной информации 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.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, 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 отделе персонала.

5.6.3. Для обеспечения внешней защиты персональных данных клиентов/(контрагентов) необходимо соблюдать ряд мер:

- порядок охраны территории, зданий, помещений;

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных клиентов .

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, клиенты/(контрагенты) и их представители могут вырабатывать совместные меры защиты персональных данных клиентов/(контрагентов).

6. Права и обязанности клиента/(контрагента)

6.1. Закрепление прав клиента/(контрагента), регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2 Клиенты/(контрагенты) и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных клиента/(контрагента), а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у исполнителя, клиент/(контрагента) имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.

- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной и семейной тайны.

6.4. Клиент/(контрагент) обязан:

- передавать исполнителю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен договорным соглашением

- своевременно сообщать исполнителю об изменении своих персональных данных.

6.5. В целях защиты частной жизни, личной и семейной тайны клиенты/(контрагенты) не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

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, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных клиента/(контрагента), несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера исполнитель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных клиента/(контрагента), 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.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки.

7.5.4. 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.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.