ПРИНЯТО

Решением Общего собрания работников ГБОУ школы № 500

Протокол № 5 от 09 января 2023 г.

УТВЕРЖДАЮ

Приказ от «09» января 2023г. № 001/1

директор ГБОУ школы № 500

_____ Базина Н.Г.

Базина Надежда Геннадьевна

Подписан: Базина Надежда Геннадьевна
DN: C=RU, S=г. Санкт-Петербург, L=Пушкин, T=Директор, O=ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ШКОЛА № 500 ПУШКИНСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА, СНИЛС=07927047091, ИНН=782092352290, E=scool500@mail.ru, G=Надежда Геннадьевна, SN=Базина, CN=Базина Надежда Геннадьевна
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место вашего подписания
Дата: 2024-05-08 10:36:23
Foxit Reader Версия: 9.6.0

Положение
о защите персональных данных при их обработке в информационных системах персональных данных ГБОУ школа № 500 Пушкинского района Санкт-Петербурга

1. Общие положения

1.1. Положение о защите персональных данных при их обработке в ГБОУ школа № 500 Пушкинского района Санкт-Петербурга (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон), от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», постановлением Правительства Российской Федерации от 01.12.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Положение регулирует отношения, связанные с обработкой персональных данных, осуществляемой ГБОУ школа № 500 Пушкинского района Санкт-Петербурга (далее ОУ) с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Настоящее Положение подлежит обязательному исполнению всеми сотрудниками ОУ.

1.3. Для целей Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

оператор персональных данных - ОУ, самостоятельно организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые

в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2. Обработка персональных данных

2.1. Обработка персональных данных осуществляется оператором персональных данных исключительно в целях реализации возложенных на него функций и должностных обязанностей, определяемых законами и иными нормативными правовыми актами в сфере обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

2.2. Объем и характер обрабатываемых персональных данных должен соответствовать целям обработки персональных данных. Недопустима обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных. Недопустимо объединение созданных для несовместимых между собой целей баз данных ИС персональных данных.

2.3. Персональные данные оператор получает от субъекта персональных данных, который принимает решение об их предоставлении и дает согласие на их обработку своей волей и в своем интересе. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В определенных Законом случаях (при обработке специальных категорий данных, биометрических данных) обработка этих данных осуществляется только с согласия в письменной форме субъекта персональных данных.

2.4. На обработку персональных данных субъекта персональных данных требуется его согласие за исключением следующих случаев:

обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия органа исполнительной власти, осуществляющего обработку персональных данных (далее - оператор);

обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

2.5. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться должностное лицо (работник), ответственное за обеспечение безопасности персональных данных.

2.6. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

2.7. Перечень персональных данных физических лиц, используемых для обработки в ИС и АИС, порядок использования, цель, периодичность и основания внесения изменений и дополнений, а также порядок хранения персональных данных устанавливаются оператором с учетом специфики своей деятельности в утвержденных операторами инструкциях, регламентирующих работы ИС и АИС.

2.8. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению по достижении целей их обработки или в случае утраты необходимости в достижении этих целей.

2.9. АИС, использующие персональные данные, включаются в реестр уполномоченного органа по защите прав физических лиц персональных данных в порядке, утвержденном Законом.

3. Обязанности и права оператора обработки персональных данных в ИС и АИС

3.1. Оператор обязан в случаях, предусмотренных Законом, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных либо его законного представителя в течение десяти рабочих дней с даты получения запроса субъекта персональных данных, либо его законного представителя.

3.2. Оператор обязан при сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 4 статьи 14 Закона.

3.3. Оператор обязан в случае, если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, до начала обработки таких персональных данных предоставить субъекту персональных данных следующую информацию:

наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

установленные Законом права субъекта персональных данных.

3.4. Оператор обязан безвозмездно предоставлять субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлению субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор в ИС и АИС, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор уведомляет субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

3.5. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.6. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

3.7. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

3.8. Оператор обязан в случае достижения цели обработки персональных данных незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае,

если обращение или запрос были направлены уполномоченным органом по защите прав физических лиц персональных данных, - также указанный орган.

3.9. Оператор обязан в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных, уведомив об этом субъекта персональных данных.

3.10. Оператор при передаче персональных данных физических лиц третьим лицам, в порядке, установленном Положением, ограничивает передаваемую информацию только теми персональными данными физических лиц, которые необходимы для выполнения третьими лицами своих функций. Передача персональных данных по телефону, факсимильной связи, электронной почте запрещается.

4. Защита персональных данных

4.1. Безопасность персональных данных достигается путем обеспечения надлежащих условий защиты персональных данных, включающих организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.2. Установка программного обеспечения на компьютер, где обрабатываются персональные данные, осуществляется уполномоченным лицом или в его присутствии.

4.3. Доступ к указанным компьютерам лиц, не допущенных к работе с персональными данными, должен быть исключен, а компьютер - защищен аппаратными или программными средствами защиты от несанкционированного использования.

4.4. Внесение изменений в перечень используемых персональных данных в базы данных ИС и АИС, при наличии оснований, предусмотренных Законом, осуществляется только по разрешению уполномоченного лица по защите информации у данного оператора.

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

4.6. Размещение информационных систем, специальное оборудование и охрана помещений, 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 или пребывания в этих помещениях посторонних лиц.

4.7. При обработке персональных данных в информационной системе должны быть обеспечены:

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

своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

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

постоянный контроль за обеспечением уровня защищенности персональных данных.

4.8. Лица, уполномоченные осуществлять обработку персональных данных, несут ответственность за защиту персональных данных в порядке, предусмотренном действующим законодательством Российской Федерации.