

от « 15 » января 2018 г.
№ 278

ПОЛИТИКА
Оператора в отношении организации обработки и
обеспечения безопасности персональных данных в
Муниципальном бюджетном общеобразовательном учреждении
«Гимназия № 91 имени М.В. Ломоносова»

1. Общие положения

1.1. Политика Оператора в отношении организации обработки и обеспечения безопасности персональных данных в МБОУ Гимназия № 91 (далее – Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в МБОУ Гимназии № 91 персональных данных, функции организации при обработке персональных данных, права субъектов персональных данных, а также реализуемые в организации требования к защите персональных данных.

1.2. Политика разработана с учетом требований Конституции РФ, законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

2. Законодательные и иные нормативные правовые акты Российской Федерации,
в соответствии с которыми определяется политика обработки персональных данных в
МБОУ Гимназия № 91

2.1. Политика Оператора в отношении организации обработки персональных данных в МБОУ Гимназия № 91 определяется в соответствии со следующими нормативными правовыми актами:

- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ № 687 от 15.09.2008 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановлением Правительства РФ № 1119 от 01.11.2012г. "Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Федеральным законом от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации";
- иными нормативными правовыми актами Российской Федерации и нормативными документами уполномоченных органов государственной власти.

2.2. В целях реализации положений Политики в МБОУ Гимназия № 91 разработаны и находятся в стадии разработки соответствующие локальные нормативные акты и иные документы, в том числе:

- приказ «О назначении лица, ответственного за организацию обработки персональных данных в МБОУ Гимназия № 91»;
- приказ «О введении в действие Положения о порядке обработки и обеспечении безопасности персональных данных в МБОУ Гимназия № 91»;

- приказ «Об утверждении перечня работников МБОУ Гимназия № 91, имеющих доступ к персональным данным работников организации в информационной системе 1С: Предприятие "Зарплата и Кадры»;
- приказ «О допуске к персональным данным», содержащий список работников, допущенных к работе с персональными данными;
- приказ «О выделении помещений для обработки персональных данных в МБОУ Гимназия № 91»;
- приказ «Об утверждении перечня информационных систем персональных данных и назначении администраторов»;
- приказ «Об утверждении Руководства пользователя и Руководства администратора информационных систем персональных данных»;
- частная модель угроз информационных систем персональных данных (ИСПДн) МБОУ Гимназия № 91, описывающая возможные угрозы персональным данным, обрабатываемым в информационных системах МБОУ Гимназия № 91, и обосновывающая уровень информационной безопасности для этих систем;
- Политика оператора в отношении организации обработки и обеспечения безопасности персональных данных в МБОУ Гимназия № 91;
- иные локальные нормативные акты и документы, регламентирующие в МБОУ Гимназия № 91 вопросы обработки персональных данных.

3. Основные термины и определения, используемые в локальных нормативных актах МБОУ Гимназия № 91, регламентирующих вопросы обработки персональных данных

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

оператор персональных данных (оператор ПДн) - юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

должностные лица - работники, состоящие в трудовых отношениях с Работодателем и имеющие право на получение, обработку, передачу в процессе работы персональных данных (руководящий состав: директор и его заместители, работники отдела кадров, бухгалтерии, члены комиссии по социальному страхованию).

третьи лица - любые лица (работники, юридические лица, должностные лица государственных органов и органов местного самоуправления, правоохранительных органов), не являющиеся стороной индивидуального трудового договора, заключенного с Работодателем в лице ее руководителя (директора) или иных уполномоченных лиц.

4. Принципы и цели обработки персональных данных

4.1. МБОУ Гимназия № 91, являясь оператором персональных данных, осуществляет обработку персональных данных работников школы и других субъектов персональных данных, не состоящих с МБОУ Гимназия № 91 в трудовых отношениях.

4.2. Обработка персональных данных в МБОУ Гимназия № 91 осуществляется с учетом необходимости обеспечения защиты прав и свобод работников организации и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

- обработка персональных данных осуществляется в МБОУ Гимназия № 91 на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечиваются их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. МБОУ Гимназия № 91 принимаются необходимые меры по удалению или уничтожению неполных или неточных персональных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем того требуют цели обработки персональных данных, если срок их хранения не установлен федеральным законом, договором, стороной которого является субъект персональных данных;
- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки, или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Персональные данные обрабатываются в МБОУ Гимназия № 91 в целях:

- обеспечения соблюдения Конституции РФ, требований Федерального закона от 29.12.2012г. № 273-ФЗ "Об образовании в Российской Федерации», законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов организации;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на МБОУ Гимназия № 91, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд РФ, в Фонд социального страхования РФ, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

- регулирования трудовых отношений с работниками организации (содействие в трудоустройстве, получение образования и продвижение по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);
- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
- подготовки, заключения, исполнения и прекращения договоров с контрагентами;
- осуществления прав и законных интересов МБОУ Гимназии № 91 в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами организации, или третьих лиц либо достижения общественно значимых целей (ведение бюджетного, налогового, оперативного, кадрового и воинского учета; взимание необходимых налогов и сборов с доходов работников в соответствии с законодательством РФ; формирование и предоставление в соответствующие органы необходимой статистической, бюджетной, налоговой и иной отчетности по установленным формам; предоставления образовательных услуг; проведения олимпиад, консультационных семинаров; направления работ сотрудников (учащихся, воспитанников) на конкурсы; ведения электронного дневника и электронного журнала успеваемости; ведения сайта ОУ; проведения мониторинга деятельности организации.

5. Перечень субъектов, персональные данные которых обрабатываются в МБОУ Гимназия № 91

5.1. В МБОУ Гимназия № 91 обрабатываются персональные данные следующих категорий субъектов:

- работников, состоящих в трудовых отношениях с МБОУ Гимназия № 91, в соответствии с трудовым законодательством;
- уволенных сотрудников МБОУ Гимназия № 91 в соответствии со сроками хранения, определенными законодательством Российской Федерации;
- физических лиц, обращающихся для зачисления в кадровый резерв МБОУ Гимназия № 91;
- получающих образование в МБОУ Гимназия № 91;
- законных представителей Субъектов, получающих образование в МБОУ Гимназия № 91;
- полученных в связи с заключением договора, стороной которого является субъект персональных данных (персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются исключительно для заключения и исполнения указанного договора);
- другие субъекты персональных данных (для обеспечения реализации целей обработки, указанных в разделе 4 Политики);

Обработка персональных данных осуществляется для достижения целей, предусмотренных пунктами 2, 5 ч. 1 ст. 6 Федерального закона «О персональных данных».

6. Перечень персональных данных, обрабатываемых в МБОУ Гимназия № 91

6.1. Перечень персональных данных, обрабатываемых в МБОУ Гимназия № 91, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами организации с учетом целей обработки персональных данных, указанных в разделе 4 Политики.

6.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, а также трансграничная передача персональных данных работников в МБОУ Гимназия № 91 не осуществляется.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7. Функции МБОУ Гимназия № 91 при осуществлении обработки персональных данных

7.1. МБОУ Гимназия № 91 при осуществлении обработки персональных данных:

- принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов организации в области персональных данных;
- принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в МБОУ Гимназия № 91;
- осуществляет ознакомление работников организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов организации в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных работников;
- публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;
- сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и/или поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;
- прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;
- совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

8. Условия обработки персональных данных в МБОУ Гимназия № 91

- 8.1. Обработка персональных данных в МБОУ Гимназия № 91 осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных;
- 8.2. МБОУ Гимназия № 91 без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом;
- 8.3. МБОУ Гимназия № 91 вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».
- 8.4. В целях внутреннего информационного обеспечения организация может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

- 8.5. Доступ к обрабатываемым в организации персональным данным разрешается только работникам организации, которые допущены к работе с ПДн на основании соответствующего приказа.

9. Перечень действий с персональными данными и способы их обработки

- 9.1. МБОУ Гимназия № 91 осуществляет сбор, запись, систематизацию, накопление, хранение, уничтожение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.
- 9.2. Обработка персональных данных в МБОУ Гимназия № 91 осуществляется следующими способами:
- неавтоматизированная обработка персональных данных;
 - автоматизированная обработка персональных данных;
 - смешанная обработка персональных данных.

10. Права субъектов персональных данных

- 10.1. Субъекты персональных данных имеют право на:
- полную информацию об их персональных данных, обрабатываемых в МБОУ Гимназия № 91;
 - доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
 - уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
 - отзыв согласия на обработку персональных данных;
 - принятие предусмотренных законом мер по защите своих прав;
 - обжалование действия или бездействия МБОУ Гимназия № 91, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;
 - осуществление иных прав, предусмотренных законодательством Российской Федерации.

11. Меры, принимаемые МБОУ Гимназия № 91 для обеспечения выполнения обязанностей оператора при обработке персональных данных

- 11.1. Меры, необходимые и достаточные для обеспечения выполнения МБОУ Гимназия № 91 обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:
- назначение лица, ответственного за организацию обработки персональных данных в школе;
 - ограничение и регламентация состава работников, имеющих доступ к персональным данным;
 - принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
 - организацию обучения и проведение методической работы с работниками МБОУ Гимназия № 91, допущенными к обработке ПДн на основании приказа по школе;
 - получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;
 - обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;

- обеспечение отдельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;
- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- парольная защита доступа пользователей к информационной системе персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на съёмных машинных носителях информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- применение в необходимых случаях средств межсетевого экранирования;
- применение в необходимых случаях средств обнаружения вторжений в корпоративную сеть, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- резервное копирование информации;
- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- размещение технических средств обработки персональных данных, в пределах охраняемой территории;
- поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности;
- установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям, включая сеть Интернет, вне пределов локальной вычислительной сети школы;
- реализация в полном объёме технических мер, утвержденных приказом ФСТЭК №21 от 18.02.2013г.;
- хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих хищение, подмену, несанкционированное копирование и уничтожение;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам МБОУ Гимназия № 91;
- иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

11.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами МБОУ Гимназия № 91, регламентирующими вопросы обеспечения безопасности ПДн при их обработке в информационных системах персональных данных школы.

12. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов МБОУ Гимназия № 91 в области персональных данных, в том числе требований к защите персональных данных

- 12.1. Контроль за соблюдением в МБОУ Гимназия № 91 законодательства Российской Федерации и локальных нормативных актов школы в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в МБОУ Гимназия № 91 законодательству Российской Федерации и локальным нормативным актам гимназии в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.
- 12.2. Внутренний контроль за соблюдением в МБОУ Гимназия № 91 законодательства Российской Федерации и локальных нормативных актов школы в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в школе.
- 12.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам гимназии, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам МБОУ Гимназия № 91 осуществляет специалист по кадрам.
- 12.4. Персональная ответственность за соблюдением требований законодательства Российской Федерации и локальных нормативных актов школы в области персональных данных в МБОУ Гимназия № 91, а также за обеспечение конфиденциальности и безопасности персональных данных, возлагается на заместителей директора, главного бухгалтера.