

Утверждаю директор
МАОУ СШ №55 г. Липецка «Лингвист»

Т.Д. Тихонова

Правила взаимодействия МАОУ СШ №55 г. Липецка «Лингвист» с уполномоченными органами.

1. Общие положения

1.1. Настоящие «Правила взаимодействия МАОУ СШ №55 г. Липецка «Лингвист» с уполномоченными органами» (далее – Правила) определяют порядок взаимодействия МАОУ СШ №55 г. Липецка «Лингвист» (далее – Оператор) с уполномоченными государственными органами, осуществляющими в соответствии с Федеральным законом № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» мероприятия по контролю (надзору) за выполнением требований, установленных Федеральным законом № 152-ФЗ «О персональных данных» и Правительством РФ, по обеспечению надлежащей организации обработки и обеспечению безопасности персональных данных, в том числе в информационных системах персональных данных (далее – уполномоченные органы).

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

1.3. Правила обязательны для исполнения всеми работниками Оператора, организующими взаимодействие с уполномоченными органами или непосредственно участвующими во взаимодействии с уполномоченными органами. Нарушение Правил влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

1.4. Настоящие Правила вступают в силу после их утверждения руководителем Оператора. Все изменения в Правила вносятся на основании решения руководителя Оператора в установленном порядке.

2. Основные понятия

2.1. В настоящих Правилах используются основные понятия, приведенные в пункте 2 «Положения МАОУ СШ №55 г. Липецка «Лингвист» об организации обработки персональных данных».

3. Обязанности Ответственного лица при взаимодействии с уполномоченными органами

3.1. Ответственность за взаимодействие с уполномоченными государственными органами, осуществляющими мероприятия по контролю над выполнением требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, несет лицо,

ответственное за организацию обработки персональных данных (далее – Ответственное лицо).

3.2. Ответственное лицо с участием юрисконсульта Оператора:

3.2.1. Своевременно подготавливает и направляет в уполномоченный орган по защите прав субъектов персональных данных уведомление о намерении Оператора осуществлять обработку персональных данных.

3.2.2. В случае изменения сведений, указанных в уведомлении о намерении осуществлять обработку персональных данных, в установленные сроки уведомляет Уполномоченный орган об этих изменениях.

3.2.3. Предоставляет Уполномоченному органу запрашиваемую при проведении проверок информацию.

3.3. Ответственное лицо регистрирует сведения о проведении проверки Уполномоченными органами в «Журнале учета проверок юридического лица, проводимых органами государственного контроля (надзора), органами муниципального контроля».

3.4. Ответственное лицо обязано обеспечить текущее хранение нижеуказанных документов в течение трех лет, а по истечении указанного срока – передать документы на архивное хранение:

- (1) требования Роскомнадзора;
- (2) уведомления Роскомнадзора, субъекта персональных данных или его представителя об устранении допущенных нарушений;
- (3) уведомления Роскомнадзора, субъекта персональных данных или его представителя о прекращении неправомерной обработки персональных данных;
- (4) ответы Роскомнадзору о неправомерности требований;
- (5) иные документы и копии иных документов, непосредственно связанные с выполнением Оператором своих обязанностей по рассмотрению требований Роскомнадзора.

4. Виды предусмотренных законодательством проверок

4.1. Уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) проводит проверки:

4.1.1. Плановые проверки (п. 21 Административного регламента проведения проверок Роскомнадзором при осуществлении контроля (надзора) за соответствием обработки персональных данных требованиям законодательства в области персональных данных).

4.1.2. Внеплановые проверки (п. 27 Административного регламента проведения проверок Роскомнадзором при осуществлении контроля (надзора) за соответствием обработки персональных данных требованиям законодательства в области персональных данных).

4.2. Федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России) проводит следующие проверки:

4.2.1. Лицензионный контроль над соблюдением лицензиатом ФСТЭК России лицензионных требований и условий (п. 14 «Положения о лицензировании деятельности по технической защите конфиденциальной информации»);

4.2.2. По обращению Роскомнадзора (п. 5.1 ч. 3 ст. 23 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»);

4.2.3. Внеплановые проверки по контролю нарушений обязательных требований (ст. 10 Федерального закона № 294-ФЗ от 26.12.2008 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»).

4.3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (ФСБ России), проводит следующие проверки:

4.3.1. Контроль над соблюдением правил пользования средствами криптографической защиты информации (п. 50 приказа ФСБ России от 09.02.2005 № 66).

4.3.2. Лицензионный контроль за соблюдением лицензиатом ФСБ России лицензионных требований и условий (п. 13 «Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» – утв. постановлением Правительства Российской Федерации от 16.04.2012 № 313).

4.3.3. По обращению Роскомнадзора (п. 5.1 ч. 3 ст. 23 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»).

4.3.4. Внеплановые проверки по контролю нарушений обязательных требований (ст. 10 Федерального закона № 294-ФЗ от 26.12.2008 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»).

5. Взаимодействие Оператора с Роскомнадзором.

5.1. Роскомнадзор, являясь уполномоченным органом по защите прав субъектов персональных данных, имеет право (ст. 23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»):

5.1.1. Запрашивать у операторов (физических или юридических лиц) информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию.

5.1.2. Осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий.

5.1.3. Требовать от оператора уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных.

5.1.4. Принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5.1.5. Обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде.

5.1.6. Направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в п. 7 ч. 3 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5.1.7. Направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных.

5.1.8. Направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

5.1.9. Привлекать к административной ответственности лиц, виновных в нарушении Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5.1.10. При получении Оператором запроса на предоставление информации Ответственное лицо проверяет законность такого запроса, после чего предоставляет запрашиваемую информацию в Роскомнадзор.

5.2. В случае получения требования Роскомнадзора об уточнении обрабатываемых Оператором (или лицом, действующим по поручению Оператора) неполных, устаревших, неточных персональных данных Ответственное лицо обязано:

5.2.1. Зафиксировать наличие требования Роскомнадзора об уточнении обработки неполных, устаревших, неточных персональных данных.

5.2.2. Осуществить блокирование указанных персональных данных с момента получения требования на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.2.3. Осуществить проверку фактов, изложенных в требовании. По результатам проверки может быть получено подтверждение или не подтверждение факта неточности персональных данных.

5.3. В случае подтверждения факта неточности персональных данных Ответственное лицо обязано:

5.3.1. Произвести/обеспечить уточнение указанных персональных данных на основании представленных сведений в течение семи рабочих дней со дня представления таких сведений.

5.3.2. Осуществить снятие блокирования указанных персональных данных.

5.3.3. В письменной форме уведомить Роскомнадзор, субъекта персональных данных или его представителя об устранении допущенных нарушений.

5.4. В случае неподтверждения факта неточности персональных данных Ответственное лицо обязано:

5.4.1. Осуществить снятие блокирования указанных персональных данных.

5.4.2. Подготовить и согласовать с юрисконсультутом Оператора ответ в письменной форме о неправомерности требования, и направить его в Роскомнадзор.

5.4.3. Совместно с юрисконсультутом Оператора подготовить предложение об обжаловании требования в порядке, установленном Административным регламентом Роскомнадзора и действующим законодательством Российской Федерации.

5.5. В случае получения требования Роскомнадзора о прекращении неправомерной обработки Оператором (или лицом, действующим по поручению Оператора) персональных данных Ответственное лицо обязано:

5.5.1. Зафиксировать наличие требования Роскомнадзора о прекращении неправомерной обработки персональных данных.

5.5.2. Осуществить блокирование указанных персональных данных с момента получения требования на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.5.3. Осуществить проверку фактов, изложенных в требовании. По результатам проверки может быть получено подтверждение или не подтверждение факта неправомерной обработки персональных данных.

5.6. В случае подтверждения факта неправомерной обработки персональных данных Ответственное лицо обязано:

5.6.1. Произвести/обеспечить прекращение неправомерной обработки персональных данных в срок, не превышающий трех рабочих дней со дня выявления неправомерной обработки персональных данных.

5.6.2. Если обеспечить правомерность обработки персональных данных невозможно - уничтожить такие персональные данные или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней со дня выявления неправомерной обработки персональных данных.

5.6.3. В письменной форме уведомить Роскомнадзор, субъекта персональных данных или его представителя об устранении допущенных нарушений. 5.7. В случае не подтверждения факта неправомерной обработки персональных данных Ответственное лицо обязано:

5.7.1. Осуществить снятие блокирования указанных персональных данных.

5.7.2. Подготовить и согласовать с юрисконсультутом Оператора ответ в письменной форме о неправомерности требования, и направить его в Роскомнадзор.

5.7.3. Совместно с юрисконсультom Оператора подготовить предложение об обжаловании требования в порядке, установленном Административным регламентом Роскомнадзора и действующим законодательством РФ.

5.8. При получении иных запросов, выходящих за рамки полномочий Роскомнадзора, Ответственное лицо должно подготовить и согласовать с юрисконсультom Оператора ответ в письменной форме о неправомерности требований, и направить его в Роскомнадзор.

5.9. При включении Оператора в план проверок Роскомнадзора Ответственное лицо незамедлительно уведомляет о предстоящей плановой проверке руководителя Оператора, всех лиц, допущенных к обработке персональных данных Оператором, проводит внутреннюю проверку защищенности персональных данных (согласно плану и методике проведения внутренних проверок).

5.10. При получении уведомления от Роскомнадзора о плановой проверке Ответственное лицо:

5.10.1. Незамедлительно уведомляет руководителя Оператора и всех лиц, допущенных к обработке персональных данных Оператором, о предстоящей проверке.

5.10.2. Проводит внутреннюю проверку защищенности персональных данных (согласно плану и методике проведения внутренних проверок).

5.11. При получении уведомления от Роскомнадзора о внеплановой проверке Ответственное лицо:

5.11.1. Запрашивает у должностного лица Роскомнадзора основания для проведения внеплановой проверки (согласно Административному регламенту Роскомнадзора).

5.11.2. Незамедлительно уведомляет руководителя Оператора и всех лиц, допущенных к обработке персональных данных Оператором, о предстоящей проверке.

5.11.3. Проводит внутреннюю проверку защищенности персональных данных (согласно плану и методике проведения внутренних проверок).

5.12. В процессе проведения плановой или внеплановой проверки Ответственное лицо:

5.12.1. Предоставляет сотрудникам Роскомнадзора информацию, необходимую для реализации проверок.

5.12.2. Контролирует соответствие процесса организации (проведения) проверки Административному регламенту Роскомнадзора.

5.12.3. Регистрирует сведения о проведении проверки в «Журнале учета проверок юридического лица, проводимых органами государственного контроля (надзора), органами муниципального контроля».

5.13. В случае выездной проверки Роскомнадзора Ответственное лицо должно ознакомиться:

(1) со служебными удостоверениями проверяющих;

(2) с копиями распоряжения/приказа о назначении проверки (под роспись), а также их получение руководителем Оператора или уполномоченным лицом. Форма приказа утверждена приказом Министерства экономического развития Российской Федерации от 30.04.2009 № 141 «О реализации положений Федерального закона «О защите прав юридических лиц и индивидуальных

предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». Проверка должна проводиться проверяющими, которые указаны в приказе;

(3) с Административным регламентом проведения проверки;

(4) с полномочиями проверяющих, а также с целями, задачами, основаниями проведения проверки, составом экспертов, со сроками и с условиями ее проведения;

(5) с Актом проверки до его подписания (по результатам проверки).

5.14. В случае совершения работниками Роскомнадзора при проведении проверки незаконных действий (в том числе нарушающих Административный регламент Роскомнадзора) или выходящих за рамки их должностных обязанностей, Ответственное лицо совместно с юрисконсультom Оператора готовит предложение об обжаловании действий (бездействий) и решения должностных лиц Роскомнадзора в порядке, установленном Административным регламентом Роскомнадзора и действующим законодательством Российской Федерации.

6. Взаимодействие Оператора с ФСТЭК России и ФСБ России

6.1. При получении Оператором запроса от ФСТЭК России или ФСБ России на предоставление информации Ответственное лицо:

6.1.1. Проверяет законность такого запроса.

6.1.2. Информирует руководителя Оператора, после чего предоставляет запрашиваемую информацию ФСТЭК России или ФСБ России.

6.2. При получении иных запросов, выходящих за рамки полномочий ФСТЭК России или ФСБ России, Ответственное лицо должно подготовить письменный ответ о незаконности предъявляемых требований.

6.3. При включении Оператора в план проверок ФСТЭК России или ФСБ России Ответственное лицо незамедлительно уведомляет о предстоящей плановой проверке руководителя Оператора, всех лиц, допущенных к обработке персональных данных Оператором, проводит внутреннюю проверку защищенности персональных данных (согласно плану и методике проведения внутренних проверок). В процессе проведения проверки ФСТЭК России или ФСБ России, Ответственное лицо:

6.3.1. Предоставляет работникам ФСТЭК России или ФСБ России информацию, необходимую для реализации проверок.

6.3.2. Регистрирует сведения о проведении проверки в «Журнале учета проверок юридического лица, проводимых органами государственного контроля (надзора), органами муниципального контроля».

6.4. В случае незаконных или выходящих за рамки должностных обязанностей действий работников ФСТЭК России или ФСБ России при проведении проверки Ответственное лицо готовит предложение об обжаловании действий (бездействий) и решения должностных лиц ФСТЭК России или ФСБ России в порядке, установленным действующим законодательством РФ.

6.5. Взаимодействие с иными уполномоченными государственными органами организуется в порядке, установленном действующим законодательством РФ.

Утверждаю директор
МАОУ СШ №55 г. Липецка «Лингвист»

Т.Д. Тихонова

**Правила МАОУ СШ №55 Г. Липецка «Лингвист» по
организации обработки и осуществления защиты персональных
данных, обрабатываемых без использования средств
автоматизации.**

1. Общие положения.

1.1. Настоящие «Правила МАОУ СШ №55 г. Липецка «Лингвист» об организации и осуществления защиты персональных данных, обрабатываемых без использования средств автоматизации» (далее – Правила) определяют порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации МАОУ СШ №55 г. Липецка «Лингвист» (далее – Оператор).

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2. Основные понятия.

2.1. В настоящих Правилах используются основные понятия, приведенные в пункте 2 «Положения МАОУ СШ №55 г. Липецка «Лингвист» об организации обработки персональных данных».

2.2. В настоящих Правилах используется дополнительное понятие:

2.2.1. Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

**3. Порядок обработки персональных данных без использования средств
автоматизации.**

3.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

3.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

3.3.1. не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

3.3.2. персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

3.3.3. документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

3.3.4. дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

3.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

3.4.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, 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;

3.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

3.4.3. 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;

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

3.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

3.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

3.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению №3 к настоящему Положению.

3.8. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

3.9. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

3.9.1. при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

3.9.2. при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.10. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

3.11. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

4.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

4.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие

несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.