

ПРИКАЗ

от 28.12.2023

№ 505-о

Об утверждении порядка оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Во исполнении требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», в рамках реализации работ по защите персональных данных, обрабатываемых в информационных системах персональных данных, во исполнение постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в соответствии постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 и требованиями Приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Порядок оценки вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (Приложение 1).

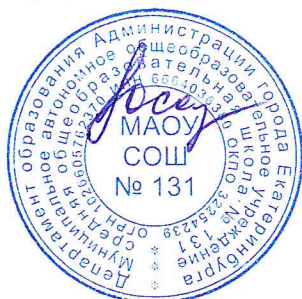
1.2. Оценку вреда (критерии оценки), который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых оператором мер (Приложение 2).

1.3. Состав комиссии по оценке вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных. (Приложению 3).

1.4. Акт оценки вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных. (Приложению 4);

4. Контроль исполнения приказа оставляю за собой.

Директор МАОУ СОШ № 131



Г.А. Осадчая

с приказом ознакомлены:

ФИО	подпись	Дата
Чкунова Светлана Александровна		28.12.2023
Ирисова Клара Викторовна		28.12.23
Мамзина Оксана Ивановна		28.12.23

**Порядок
оценки вреда, который может быть причинен субъекту (субъектам) персональных
данных в случае нарушения требований по обработке и обеспечению безопасности
персональных данных**

1. Общие положения

1.1. Настоящий Порядок оценки вреда субъектам персональных данных (далее – Порядок) определяет правила оценки вреда, который может быть причинён субъекту персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в муниципальном автономном общеобразовательном учреждении средняя общеобразовательная школа № 131 (далее – Учреждение), а также форму акта оценки вреда.

1.2. Настоящий Порядок принят в целях обеспечения соответствия процессов обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Порядок предназначен для следующих категорий сотрудников Учреждения:

- сотрудник, ответственный за организацию обработки персональных данных;
- сотрудники, которым Учреждением поручено обрабатывать персональные данные.

Под сотрудниками в настоящем Порядке понимаются лица, состоящие в трудовых или договорных отношениях с Учреждением.

1.4. Порядок разработан в целях реализации требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с требованиями Приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

1.5. Порядок действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим. Порядок подлежит пересмотру в случае изменения требований законодательства, изменения оценки рисков информационной безопасности. Изменения в документ вносятся путём издания новой версии и ознакомления с ним сотрудников, а также лиц, осуществляющих обработку персональных данных.

2. Порядок проведения оценки вреда субъекту персональных данных

2.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2. Оценка уровня вреда, который может быть причинен субъекту персональных данных в случае реализации угроз безопасности информации, проводится путём оценки тяжести последствий от нарушения каждого из свойств безопасности персональных данных в отдельности.

2.3. Вводятся три вербальных градации показателя уровня вреда:

- вред отсутствует – если нарушение свойств безопасности персональных данных не может привести к каким-либо негативным последствиям для субъекта персональных данных;
- низкий уровень вреда – если нарушение свойств безопасности персональных данных может привести к незначительным негативным последствиям для субъекта персональных данных;
- средний уровень вреда – если нарушение свойств безопасности персональных данных может привести к негативным последствиям для субъекта персональных данных;
- высокий уровень вреда – если нарушение свойств безопасности персональных данных может привести к значительным негативным последствиям для субъекта персональных данных.

2.4. Субъекту персональных данных может быть причинён вред в форме:

Убытков – расходов, которые лицо, чьё право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

Морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

2.5. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

2.5.1. Высокую степень в случаях:

- обработки сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;
- обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;
- обработки персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации;
- обезличивания персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований;

- поручения иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации;

- сбора персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.

2.5.2. Среднюю степень в случаях:

- распространения персональных данных на официальном сайте в информационно-телекоммуникационной сети Интернет, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных

федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;

- обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;

- продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор;

- получения согласия на обработку персональных данных посредством реализации на официальном сайте в информационно-телекоммуникационной сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;

- осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

2.5.3. Низкую степень в случаях:

- ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- назначения в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником оператора.

2.6. В случае если по итогам проведённой оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии подпунктами 2.5.1–2.5.3 пункта 2.5 настоящего Порядка могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

2.7. Оценка вреда субъекту персональных данных осуществляется ответственным за организацию обработки персональных данных либо комиссией, образуемой Учреждением.

2.8. По результатам оценки степени вреда субъекту персональных данных оформляется акт оценки вреда субъекту персональных данных (далее – Акт).

2.9. Акт может быть оформлен на бумажном носителе, подписанном собственноручно лицом (лицами), производившими оценку, либо в виде электронного документа, подписанного в соответствии электронной подписью.

2.10. Акт оценки вреда должен содержать:

- а) фамилию, имя, отчество (при наличии) и адрес оператора;
- б) дату издания акта оценки вреда;
- в) дату проведения оценки вреда;
- г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;
- д) степень вреда, которая может быть причинена субъекту персональных данных, определённая в соответствии с методикой оценки вреда, указанной в разделе 2.5 настоящего регламента.

2.11. Оценка вреда подлежит пересмотру не реже 1 раза в год.

Критерии оценки степени вреда субъектам персональных данных

Высокая степень	
- обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных	НЕТ
- обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных	НЕТ
- обработка персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации	НЕТ
- обезличивание персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований	НЕТ
- поручение иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации	НЕТ
- сбор персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.	НЕТ
Средняя степень	
- распространение персональных данных на официальном сайте в информационно-телекоммуникационной сети Интернет, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных	ДА
- обработка персональных данных в дополнительных целях, отличных от первоначальной цели сбора	НЕТ
- продвижение товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор	НЕТ
- получение согласия на обработку персональных данных посредством реализации на официальном сайте в информационно-телекоммуникационной сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных	ДА

<p>- осуществление деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой</p>	<p>НЕТ</p>
<p>Низкая степень</p>	
<p>- ведение общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;</p>	<p>НЕТ</p>
<p>- назначение в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником оператора</p>	<p>НЕТ</p>

Состав комиссии по оценке вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых оператором мер

ФИО	Должность	Функционал в комиссии
Чикунова Светлана Александровна	Заместитель директора по ВР	Председатель комиссии
Ирисова Клара Викторовна	Учитель	Член комиссии
Мамзина Оксана Ивановна	Учитель	Член комиссии

УТВЕРЖДАЮ
Директор МАОУ СОШ № 131
_____ Г.А. Осадчая
« ____ » _____ 20__ г.

АКТ

оценки вреда, который может быть причинён субъектам персональных
данных в случае нарушения Федерального закона «О персональных данных»

« ____ » _____ 20__ г.

№ ____

Настоящий Акт составлен ответственным за организацию обработки персональных
данных/комиссией, действующей на основании приказа от « ____ » _____ 20__ г.
№ ____, в составе:

председатель комиссии: _____ /ФИО, должность;
члены комиссии: _____ /ФИО, должность;
_____ /ФИО, должность.

Комиссия « ____ » _____ 20__ г. провела оценку вреда, который может быть
причинён субъектам персональных данных в случае нарушения Федерального закона «О
персональных данных», и установила следующее:

1. Персональные данные субъектов персональных данных обрабатываются в
следующих информационных системах:

- Федеральная информационная система «Федеральный реестр сведений документов об
образовании и (или) о квалификации, документах об обучении» (ФИС ФРДО);
- Федеральная информационная система оценки качества образования (ФИС ОКО);
- Официальный сайт для размещения информации о государственных (муниципальных)
учреждениях;
- Региональный сегмент Единой федеральной межведомственной системы учета
контингента – АИС;
- Автоматизированная система бухгалтерского учета.

2. МАОУ СОШ № 131 осуществляет обработку персональных данных,
предполагающих получение письменного согласия на обработку.

3. Степень вреда, который может быть причинён субъектам персональных данных,
- _____.

4. Защищённость информации в МАОУ СОШ № 131 соответствует требованиям,
установленным постановлением Правительства РФ от 01.11.2012 № 1119.

Председатель комиссии _____ / _____ /

Члены комиссии _____ / _____ /
_____ / _____ /