УТВЕРЖДЕНЫ

приказом муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения»

Каменского района Пензенской области

от 27.06.2025 №15-ос

**Правила**

**об оценке вреда, который может быть причинен субъектам персональных данных, в случае нарушения Федерального закона «О персональных данных»**

**1. Общие положения**

1.1 Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных и Приказом Роскомнадзора от 27.10.2022 г. N 178 "Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных, в случае нарушения Федерального закона "О персональных данных".

1.2. Настоящие Правила об оценке вреда, который может быть причинен субъектам персональных данных, в случае нарушения федерального закона о персональных данных (далее - Правила) определяет порядок оценки вреда, который может быть причинен субъектам персональных данных при осуществлении деятельности МБУ «КЦСОН» Каменского района (далее - Оператор) в случае нарушения Федерального закона от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных).

**2. Основные понятия**

2.1. В настоящих Правилах используются следующие основные понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

3) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

4) целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;

5) доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

6) убытки - расходы, которые лицо, чье 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;

7) моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;

8) оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3**. Методика оценки возможного вреда субъектам персональных данных**

3.1. 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.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

1) неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

2) неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

3) неправомерное изменение персональных данных является нарушением целостности персональных данных;

4) нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;

5) нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;

6) обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;

7) неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

8) принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинен вред в форме:

1) убытков - расходов, которые лицо, чье 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;

2) 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.

3.4. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных:

1) высокую в случаях:

а) 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;

б) обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

в) 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;

г) 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, не предусмотренных пунктом 9 части 1 статьи 6 Закона о персональных данных;

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

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

2) среднюю в случаях:

а) распространения персональных данных на официальном сайте в информационно-телекоммуникационной сети "Интернет" оператора, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;

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

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

г) 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;

д) 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.

3) низкую в случаях:

а) ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Закона о персональных данных;

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

3.5. Результаты оценки вреда оформляются актом оценки вреда. Акт оценки вреда должен содержать:

1) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;

2) дату издания акта оценки вреда;

3) дату проведения оценки вреда;

4) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;

5) степень вреда, которая может быть причинена субъекту персональных данных, в соответствии с пунктом 3.4 настоящих Правил.

3.6 Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

3.7 В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии пунктом 3.4 настоящих Правил могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

4. **Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых мер**

4.1. Комиссия проводит оценку возможного вреда, который может быть причинен субъектам персональных данных, устанавливая уровень возможного вреда, в соответствии с пунктом 3.4 настоящих Правил.

4.2 По результатам оценки возможного вреда субъекту персональных данных комиссией составляется акт оценки возможного вреда субъектам персональных данных (приложение 1 к настоящим Правилам), подписывается членами комиссии, утверждается директором МБУ «КЦСОН» Каменского района. Допускается оформление одного акта на несколько субъектов персональных данных.

Приложение 1

к Правилам об оценке вреда, который

может быть причинен субъектам

персональных данных, в случае

нарушения Федерального закона

«О персональных данных»

Форма акта оценки возможного вреда субъектам персональных данных

"УТВЕРЖДАЮ"

Директор МБУ «КЦСОН»

Каменского района

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**АКТ**

**оценки возможного вреда субъектам персональных данных**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Основание: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Составлен комиссией:

Председатель -

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

"\_\_\_\_ " 20\_\_\_\_ г. комиссия провела оценку возможного вреда, который может быть причинен оператором - муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения» Каменского района Пензенской области, <...> субъекту персональных данных при нарушении Федерального закона от 27.07.2006 г N 152-ФЗ "О персональных данных"

По результатам оценки установлено, уровень потенциального вреда \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, исходя из того, что\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Председатель комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_