

Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"

Приказ · № 178 · от 27.10.2022 · Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций · Действует без изменений

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

ПРИКАЗ

Москва

27 октября 2022 г. № 178

Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"

Зарегистрирован Минюстом России 28 ноября 2022 г.

Регистрационный № 71166

В соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233), абзацем вторым пункта 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431), приказываю:

1. Утвердить прилагаемые Требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных".
2. Настоящий приказ вступает в силу с 1 марта 2023 г. и действует до 1 марта 2029 г.

Руководитель А.Ю.Липов

Утверждены

приказом Федеральной службы
по надзору в сфере связи,
информационных технологий
и массовых коммуникаций
от 27 октября 2022 г. № 178

Требования

к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"

1. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" 1 (далее - оценка вреда), осуществляется ответственным за организацию обработки персональных данных либо комиссией, образуемой оператором (далее - оператор) 2 .
2. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных:
 - 2.1. Высокую 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, интимной жизни, 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 3 ;

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 4 ;

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

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

2.2. Среднюю в случаях:

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;

обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора; продвижения товаров, работ, услуг на рынке путем 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 5 .

2.3. Низкую в случаях:

ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Закона о персональных данных 6 ;

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

3. Результаты оценки вреда оформляются актом оценки вреда.

4. Акт оценки вреда должен содержать:

- а) наименование или 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, в соответствии с подпунктами 2.1 - 2.3 пункта 2 настоящих Требований.

5. Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью 7, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

6. В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии подпунктами 2.1 - 2.3 пункта 2 настоящих Требований могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

1 Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233 (далее - Закон о персональных данных).

2 Пункт 2 статьи 3 Закона о персональных данных (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701).

3 Пункт 5 части 1 статьи 6 Закона о персональных данных (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233).

4 Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701.

5 Часть 2 статьи 5 Закона о персональных данных (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701).

6 Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701.

7 Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2022, № 29, ст. 5306).