Частное образовательное учреждение
высшего образования
«Курский институт менеджмента, экономики и бизнеса»

УТВЕРЖДАЮ
Ректор ЧОУ ВО «Курский институт
менеджмента, экономики и бизнеса»
приказ № 01.01-03/53 от 27.04.2024

_____В.М. Окороков
Рассмотрено и принято на заседании
Ученого совета
протокол № 5 от 27.04.2024

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

Курск, 2024

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Оператор – государственный орган, муниципальный орган, юридическое или физическое 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 (ИСПДн) – совокупность содержащихся в базах данных персональных данных и

обеспечивающих их обработку информационных технологий и технических средств.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Регламент оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (далее – Регламент) определяет единый и обязательный порядок и методику оценки вреда, который может быть причинён субъекту персональных в случае нарушения требований Федерального закона «О персональных данных» Частным образовательным учреждением высшего образования «Курский институт менеджмента, экономики и бизнеса» (далее – Оператор, Организация). Настоящий Регламент принят в целях обеспечения соответствия деятельности Оператора требованиям Федерального закона «О персональных данных». Настоящий документ обязаны знать и использовать в работе члены комиссии по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

3. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оценка возможного вреда субъекту персональных данных осуществляется комиссией по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», назначенной приказом ректора Частного образовательного учреждения высшего образования «Курский институт менеджмента, экономики и бизнеса», в соответствии с методикой, описанной в разделе 4 настоящего Регламента.

По результатам оценки уровня возможного вреда субъекту персональных данных оформляется акт оценки возможного вреда субъекту персональных данных.

Допускается оформление одного акта на несколько категорий субъектов персональных данных.

4. МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекту персональных данных может быть причинён вред в форме:

а) 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;

б) 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. 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. Оценка степени вреда, который может быть причинен субъекту персональных данных осуществляется в соответствии с приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»». Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных.

Высокая степень вреда устанавливается в случаях:

- обработки Оператором 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 Оператором 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 Оператором 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, не предусмотренных пунктом 9 части 1 статьи 6 Закона о персональных данных;

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

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

Средняя степень вреда устанавливается в случаях:

- распространения персональных данных на официальном сайте Оператора в 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 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 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.

Низкая в случаях:

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

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

5. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ОЦЕНКИ ВРЕДА

Результаты оценки вреда оформляются актом оценки вреда.

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, определенная в соответствии с методикой оценки вреда, указанной в разделе 4 настоящего Регламента. 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. В случае если по итогам проведенной оценки вреда установлено,

что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии с методикой оценки вреда могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

6. ПЕРЕСМОТР РЕГЛАМЕНТА

Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

– при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;

– при существенном изменении процессов обработки персональных данных Организации.