Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 12 июня 2023 года № 179/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 15 июня 2023 года № 32810.

В соответствии с подпунктом 2-3) пункта 1 статьи 27-1 Закона Республики Казахстан "О персональных данных и их защите" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных.

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан *Б. Мусин*

Утверждены приказом
Министр цифрового
развития, инноваций
и аэрокосмической
промышленности
Республики Казахстан
от 12 июня 2023 года № 179/НҚ

Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных

Глава 1. Общие положения

1. Настоящие Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных (далее – Правила) разработаны в соответствии с подпунктом 2-3) пункта 1 статьи 27-1 Закона Республики Казахстан "О персональных данных и их защите" (далее – Закон) и определяют порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных.

2. В настоящих Правилах используются следующие основные понятия:

1) персональные данные – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе;

2) блокирование персональных данных – действия по временному прекращению сбора, накопления, изменения, дополнения, использования, распространения, обезличивания и уничтожения персональных данных;

3) сбор персональных данных – действия, направленные на получение персональных данных;

4) уничтожение персональных данных – действия, в результате совершения которых невозможно восстановить персональные данные;

5) обезличивание персональных данных – действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно;

6) база, содержащая персональные данные (далее – база) – совокупность упорядоченных персональных данных;

7) собственник базы, содержащей персональные данные (далее – собственник) – государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные;

8) оператор базы, содержащей персональные данные (далее – оператор) – государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;

9) защита персональных данных – комплекс мер, в том числе правовых, организационных и технических, осуществляемых в целях, установленных Законом;

10) уполномоченный орган в сфере защиты персональных данных (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство в сфере защиты персональных данных;

11) обработка персональных данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных;

12) нарушение безопасности персональных данных – нарушение защиты персональных данных, повлекшее незаконное распространение, изменение, и уничтожение, несанкционированное распространение передаваемых, хранимых или иным образом обрабатываемых персональных данных или несанкционированный доступ к ним;

13) субъект персональных данных (далее – субъект) – физическое лицо, к которому относятся персональные данные;

14) общедоступные персональные данные – персональные данные или сведения, на которые в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта;

15) персональные данные ограниченного доступа – персональные данные, доступ к которым ограничен законодательством Республики Казахстан;

16) третье лицо – лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними (ним) обстоятельствами или правоотношениями по сбору, обработке и защите персональных данных;

17) электронные информационные ресурсы – данные в электронно-цифровой форме , содержащиеся на электронном носителе и в объектах информатизации;

18) обследование обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах (далее – обследование), – оценка применяемых мер безопасности и защитных действий при осуществлении обработки, хранения, распространения и защите персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах.

Иные понятия, используемые в настоящих Правилах, применяются в соответствии с Законом и Законом Республики Казахстан "Об информатизации".

Сноска. Пункт 2 – в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 28.02.2024 № 100/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Глава 2. Порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных

3. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих возможность несанкционированного, в том числе случайного, доступа к персональным данным при их сборе и обработке, результатом

которого могут стать уничтожение, изменение, блокирование, копирование, несанкционированное предоставление третьим лицам, несанкционированное распространение персональных данных, а также иные неправомерные действия.

4. Защита персональных данных осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях:

1) реализации прав на неприкосновенность частной жизни, личную и семейную тайну;

2) обеспечения их целостности и сохранности;

3) соблюдения их конфиденциальности;

4) реализации права на доступ к ним;

5) предотвращения незаконного их сбора и обработки.

5. Для обеспечения защиты персональных данных необходимо:

1) выделение бизнес-процессов, содержащих персональные данные;

2) разделение персональных данных на общедоступные и ограниченного доступа;

3) определение перечня лиц, осуществляющих сбор и обработку персональных данных либо имеющих к ним доступ;

4) назначение лица, ответственного за организацию обработки персональных данных в случае, если собственник и (или) оператор являются юридическими лицами. Обязанности лица, ответственного за организацию обработки персональных данных, указаны в пункте 3 статьи 25 Закона. Действие настоящего подпункта 4) не распространяется на обработку персональных данных в деятельности судов.

5) установление порядка доступа к персональным данным.

6) утверждение документов, определяющих политику оператора в отношении сбора , обработки и защиты персональных данных;

7) по запросу уполномоченного органа в рамках рассмотрения обращений физических и юридических лиц представление информации о способах и процедурах, используемых для обеспечения соблюдения собственником и (или) оператором требований Закона;

8) в течение одного рабочего дня с момента обнаружения нарушения безопасности персональных данных уведомление уполномоченного органа о данном нарушении с указанием контактных данных лица, ответственного за организацию обработки персональных данных (при наличии);

9) в случае взаимодействия с объектами информатизации государственных органов и (или) государственных юридических лиц, содержащими персональные данные, обеспечение интеграции собственных объектов информатизации, задействованных в процессах сбора и обработки персональных данных, с государственным сервисом контроля доступа к персональным данным, за исключением случаев, предусмотренных подпунктами 1), 2), 9) и 9-2) статьи 9 Закона.

При сборе и обработке персональных данных в объектах информатизации дополнительно необходимо обеспечение сохранности носителей персональных данных.

Сноска. Пункт 5 – в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 28.02.2024 № 100/НҚ (порядок введения в действие см. п.4).

6. Иные особенности защиты персональных данных при их сборе и обработке в объектах информатизации устанавливаются в соответствии с законодательством Республики Казахстан об информатизации.

7. Собственник и (или) оператор при обработке персональных данных ограниченного доступа:

1) устанавливают цели обработки персональных данных ограниченного доступа. Персональные данные ограниченного доступа используются в соответствии с декларируемыми целями.

2) определяют порядок обработки, распространения и доступа к персональным данным ограниченного доступа;

3) определяют порядок блокирования персональных данных ограниченного доступа , относящихся к субъекту, при обращении субъекта.

Собственник и (или) оператор, а также третье лицо при обработке персональных данных ограниченного доступа:

1) определяют перечень лиц, имеющих доступ к персональным данным ограниченного доступа;

2) оповещают уполномоченный орган об инцидентах информационной безопасности, связанных с незаконным доступом к персональным данным ограниченного доступа;

3) обеспечивают установку средств защиты информации, обновлений программного обеспечения на технических средствах, осуществляющих обработку персональных данных ограниченного доступа;

4) обеспечивают ведение журнала событий систем управления базами;

5) обеспечивают ведение журнала действий пользователей, имеющих доступ к персональным данным ограниченного доступа;

6) применяют средства контроля целостности персональных данных ограниченного доступа;

7) обеспечивают передачу персональных данных ограниченного доступа иным лицам по защищенным каналам связи и (или) с применением шифрования и при наличии согласия субъекта персональных данных, если иное не предусмотрено законодательством Республики Казахстан;

8) выделяют бизнес-процессы, содержащие персональные данные ограниченного доступа;

9) обеспечивают применение средств криптографической защиты информации для надежного хранения персональных данных ограниченного доступа;

10) применяют средства идентификации и (или) аутентификации пользователей при работе с персональными данными ограниченного доступа.

Сноска. Пункт 7 с изменением, внесенным приказом Министра цифрового развития , инноваций и аэрокосмической промышленности РК от 28.02.2024 № 100/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

8. Сбор и обработка персональных данных ограниченного доступа осуществляются посредством объектов информатизации, размещенных на территории Республики Казахстан.

Хранение и передача персональных данных ограниченного доступа осуществляются с использованием средств криптографической защиты информации, имеющих параметры не ниже третьего уровня безопасности согласно стандарту Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования".

Требования настоящего пункта не распространяются на случаи трансграничной передачи данных.