

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

***Утративший силу***

Постановление Правительства Республики Казахстан от 3 сентября 2013 года № 909. Утратило силу постановлением Правительства Республики Казахстан от 13 июля 2023 года № 559.

      Сноска. Утратило силу постановлением Правительства РК от 13.07.2023 № 559 (вводится в действие со дня его первого официального опубликования).

      Примечание РЦПИ!

      Вводится в действие с 25 ноября 2013 года.

      В соответствии с подпунктом 4) статьи 26 Закона Республики Казахстан "О персональных данных и их защите" Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

      Сноска. Преамбула - в редакции постановления Правительства РК от 17.03.2023 № 228 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

      2. Настоящее постановление вводится в действие с 25 ноября 2013 года и подлежит официальному опубликованию.

|  |  |
| --- | --- |
| Премьер-Министр |  |
| Республики Казахстан | С. Ахметов |

|  |  |
| --- | --- |
|  | Утверждены постановлением Правительства Республики Казахстан от 3 сентября 2013 года № 909 |

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

      Сноска. Правила - в редакции постановления Правительства РК от 18.01.2021 № 12 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

**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 4) статьи 26 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.

      Сноска. Пункт 1 - в редакции постановления Правительства РК от 17.03.2023 № 228 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

      13) 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;

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

      15) 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;

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

      17) 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 с изменениями, внесенными постановлениями Правительства РК от 30.04.2021 № 285 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 26.10.2022 № 849 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 17.03.2023 № 228 (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. Исключен постановлением Правительства РК от 17.03.2023 № 228 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

      4. 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.

      5. 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.

      6. Исключен постановлением Правительства РК от 17.03.2023 № 228 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

      7. 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 подпункта 4) настоящего пункта 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.

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

      Сноска. Пункт 7 с изменениями, внесенными постановлением Правительства РК от 14.04.2022 № 219 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

      9. 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 в сфере защиты персональных данных 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.

      10. 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 данного пункта не распространяются на случаи трансграничной передачи данных.

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан