О внесении изменений и дополнений в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2022 года № 144/НҚ "Об утверждении Правил функционирования государственного сервиса контроля доступа к персональным данным"

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 17 июня 2025 года № 299/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 18 июня 2025 года № 36295

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2022 года № 144/НҚ "Об утверждении Правил функционирования государственного сервиса контроля доступа к персональным данным" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 27963) следующие изменения и дополнения:

в заголовок вносится изменение на казахском языке, текст на русском языке не меняется;

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 7-2) пункта 1 статьи 27-1 Закона Республики Казахстан "О персональных данных и их защите" и подпунктом 268-1) пункта 15 Положения о Министерстве цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 12 июля 2019 года №501, **ПРИКАЗЫВАЮ:**";

в Правилах функционирования государственного сервиса контроля доступа к персональным данным, утвержденных указанным приказом:

пункт 1 изложить в следующей редакции:

"1. Настоящие Правила функционирования государственного сервиса контроля доступа к персональным данным (далее – Правила) разработаны в соответствии с подпунктом 7-2) пункта 1 статьи 27-1 Закона Республики Казахстан "О персональных данных и их защите" (далее – Закон), подпунктом 268-1) пункта 15 Положения о Министерстве цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 12 июля 2019 года № 501 и определяют порядок функционирования государственного сервиса контроля доступа к персональным данным.";

пункт 2 изложить в следующей редакции:

"2. В настоящих Правилах используются следующие основные понятия:

1) SMS-шлюз Единого контакт-центра "1414" – компонент "электронного правительства" для отправления и приема SMS-сообщений;

2) токен аутентификации - электронный ключ, в виде набора определенного количества цифр и букв, предназначенный для дополнительной проверки подлинности инициатора и (или) оператора;

3) банк - юридическое лицо, являющееся коммерческой организацией, которое в соответствии с Законом Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" правомочно осуществлять банковскую деятельность;

4) инициатор – информационная система, инициирующая запрос на доступ к персональным данным;

5) токен верификации – электронный ключ в виде набора определенного количества цифр и букв, предназначенный для подтверждения получения согласия инициатором и (или) оператором от субъекта персональных данных;

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

7) государственный сервис контроля доступа к персональным данным (далее – государственный сервис) – услуга, обеспечивающая информационное взаимодействие собственников и (или) операторов, третьих лиц с субъектом персональных данных и уполномоченным органом при доступе к персональным данным, содержащимся в объектах информатизации государственных органов и (или) государственных юридических лиц, включая получение от субъекта персональных данных согласия на сбор, обработку персональных данных или их передачу третьим лицам;

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

9) 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;

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

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

12) токен безопасности – электронный ключ в виде набора определенного количества цифр и букв в формате JWT, предназначенный для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца;

13) услугодатель – центральные государственные органы, загранучреждения Республики Казахстан, местные исполнительные органы областей, городов республиканского значения, столицы, районов, городов областного значения, акимы районов в городе, городов районного значения, поселков, сел, сельских округов, а также физические и юридические лица, оказывающие государственные услуги в соответствии с законодательством Республики Казахстан;

14) база мобильных граждан (далее – БМГ) – единая база абонентских номеров сети сотовой связи пользователей "электронного правительства";

15) SMS-шлюз Единого контакт-центра "1414" информационной системы " Мобильное правительство" – компонент "электронного правительства" для отправления и приема SMS-сообщений;

16) проактивная услуга – государственная услуга, оказываемая без заявления услугополучателя по инициативе услугодателя;

17) оператор информационно-коммуникационной инфраструктуры "электронного правительства" (далее – оператор "электронного правительства") – юридическое лицо, определяемое Правительством Республики Казахстан, на которое возложено обеспечение функционирования закрепленной за ним информационно-коммуникационной инфраструктуры "электронного правительства";

18) шлюз "электронного правительства" (далее – ШЭП) – информационная система, предназначенная для интеграции объектов информатизации "электронного правительства" с иными объектами информатизации "электронного правительства";

пункт 4 изложить в следующей редакции:

"4. При соответствии информационных систем единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденным постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 и наличии протоколов испытаний на соответствие требованиям информационной безопасности, процесс получения доступа к персональным данным осуществляется следующими способами:

1) посредством отправки инициатором и (или) оператором запроса на доступ к персональным данным и получение ответа от субъекта SMS-сообщения через SMS-шлюз Единого контакт-центра "1414" о согласии (отказ) на сбор и (или) обработку персональных данных или их передачу третьим лицам (далее – запрос/ответ через Единый контакт-центр "1414");

2) посредством отправки инициатором и (или) оператором, в том числе банками и организациями, имеющими согласование с уполномоченным органом в сфере защиты персональных данных, запроса на доступ к персональным данным и получение ответа от субъекта в информационной системе инициатора и (или) оператора о согласии (отказ) на сбор и (или) обработку персональных данных или их передачу третьим лицам (далее – запрос/ответ средствами инициатора и (или) оператора);

3) посредством отправки инициатором, оказывающим проактивные услуги запроса на доступ к персональным данным и получение ответа от субъекта в информационной системе инициатора согласии (отказ) на сбор и (или) обработку персональных данных или их передачу третьим лицам (далее – запрос/ответ средствами инициатора, оказывающим проактивные услуги);

4) посредством отправки инициатором, в соответствии со статьей 9 Закона Республики Казахстан "О персональных данных и их защите" запроса на доступ к персональным данным и получение ответа от субъекта в информационной системе инициатора согласии (отказ) на сбор и (или) обработку персональных данных или их передачу третьим лицам (далее – запрос/ответ в режиме протоколирования);

5) посредством отправки инициатором и (или) оператором запроса в Государственный сервис в виде SMS-сообщения с буквенно-цифровым или цифровым одноразовым кодом, отправленным через информационную систему "Мобильное правительство" на доступ к персональным данным и получение ответа в виде SMS-сообщения с буквенно-цифровым или цифровым одноразовым кодом в Государственный сервис согласии (отказ) на сбор и (или) обработку персональных данных или их передачу третьим лицам (далее – запрос/ответ в Государственный сервис осуществляются посредством SMS-сообщений, отправленных через информационную систему "Мобильное правительство");";

пункт 6 изложить в следующей редакции:

"6. Процесс получения доступа к персональным данным посредством запроса/ответа средствами инициатора и (или) оператора осуществляется согласно подпунктам 1), 2) и 3) настоящего пункта.";

Пункт 6 дополнить подпунктами 1), 2) и 3) следующего содержания:

"1) процесс получения доступа к персональным данным посредством запроса/ответа средствами инициатора, оказывающим проактивные услуги, состоит из:

получения инициатором согласия у субъекта на доступ к его персональным данным следующими способами:

системы биометрии;

электронные цифровые подписи;

бумажные носители информации;

отправки инициатором запроса на доступ к персональным данным к государственному сервису с открытым ключом электронно-цифровой подписи (далее – эцп) в токене верификации и кода проактивной услуги (предоставляется инициатором);

проверки государственным сервисом наличия токена верификации в запросе на доступ к персональным данным;

проверки государственным сервисом подписи токена верификации на соответствие, представленного эцп;

проверки государственным сервисом соответствия бизнес-идентификационного номера и кода проактивной услуги;

проверки государственным сервисом соответствия бизнес-идентификационного номера в токене верификации организации и бизнес-идентификационного номера, указанный в запросе на доступ к персональным данным;

проверки государственным сервисом на соответствие возможным способам получения доступа к персональным данным и указанным в токене верификации;

проверки государственным сервисом даты формирования токена верификации;

формирования государственным сервисом токена безопасности на период оказания проактивной услуги при прохождении всех проверок токена верификации;

отправки инициатором и (или) оператором запроса на доступ к персональным данным с включенным в запрос токеном безопасности к собственнику;

проверки собственником токена безопасности на соответствие запросу и сроку действия;

обработки запроса и отправление ответа собственником инициатору и (или) оператору;

2) процесс получения доступа к персональным данным посредством запроса/ответа в режиме протоколирования, состоит из:

отправки инициатором запроса на доступ к персональным данным к государственному сервису с открытым ключом эцп в токене верификации (с пометкой об отсутствии полученного согласия) и кода из справочника оснований получения доступа к персональным данным без получения согласия субъекта персональным данных;

проверки государственным сервисом наличия токена верификации в запросе на доступ к персональным данным;

проверки государственным сервисом подписи токена верификации на соответствие, представленного эцп;

проверки государственным сервисом бизнес-идентификационного номера на предмет возможности получения токена безопасности в режиме протоколирования;

проверки государственным сервисом соответствия бизнес-идентификационного номера в токене верификации организации и бизнес-идентификационного номера, указанный в запросе на доступ к персональным данным;

проверки государственным сервисом даты формирования токена верификации;

формирования государственным сервисом токена безопасности на период 15 минут при прохождении всех проверок токена верификации;

отправки инициатором и (или) оператором запроса на доступ к персональным данным с включенным в запрос токеном безопасности к собственнику;

проверки собственником токена безопасности на соответствие запросу и сроку действия;

обработки запроса и отправление ответа собственником инициатору и (или) оператору;

3) процесс получения доступа к персональным данным посредством запроса/ответа в государственный сервис осуществляются посредством sms-сообщений, отправленных через информационную систему "мобильное правительство", состоит из:

отправки инициатором и (или) оператором запроса на доступ к персональным данным к государственному сервису;

проверки государственным сервисом наличия запроса на доступ к персональным данным в процессе обработки;

при наличии запроса на доступ к персональным данным в процессе обработки, государственный сервис отправляет статус "ожидание ответа от субъекта".

при отсутствии запроса на доступ к персональным данным в процессе обработки, государственный сервис отправляет запрос на получение абонентского номера сети сотовой связи субъекта к бмг.

при отсутствии абонентского номера сети сотовой связи субъекта в бмг, субъект осуществляет регистрацию на веб-портале "электронного правительства".

после получения абонентского номера сети сотовой связи субъекта от бмг, государственный сервис отправляет запрос на доступ к персональным данным субъекту посредством sms-сообщения с буквенно-цифровым или цифровым одноразовым кодом через информационную систему "мобильное правительство";

после получения ответа от государственного сервиса статуса "ожидание ответа от субъекта" и идентификатора запроса государственного сервиса, инициатор и (или) оператор отправляет повторный запрос с идентификатором запроса государственного сервиса;

отправка токена безопасности государственным сервисом при повторном запросе доступа к персональным данным инициатором и (или) оператором с буквенно-цифровым или цифровым одноразовым кодом, соответствующим отправленному коду через информационную систему "мобильное правительство";

отправки инициатором и (или) оператором запроса на доступ к персональным данным с включенным в запрос токеном безопасности к собственнику;

проверки собственником токена безопасности на соответствие запросу и сроку действия;

обработки запроса и отправление ответа собственником инициатору и (или) оператору;";

в пункте 7:

подпункты 5), 6), 7), 8) и 9) изложить в следующей редакции:

"5) идентификатор справочника, сформированный государственным сервисом, который включает следующие данные, предоставленные инициатором и (или) оператором:

наименование услуг, в рамках которых будет получен доступ к персональным данным;

список идентификаторов сервисов "ServiceID" ШЭП;

период оказания услуги;

время хранения и обработки персональных данных;

6) признак способа отправки запроса и получения ответа от субъекта;

7) идентификатор справочника, сформированный государственным сервисом, с причинами получения согласия способами 3 и 4 в соответствии с пунктом 4 настоящих правил;

8) токен верификации указывается при выборе способа 2, 3 и 4 в соответствии с пунктом 4 настоящих правил;

9) токен аутентификации;";

подпункт 10) исключить;

дополнить подпунктом 11) следующего содержания:

"11) данные для проверки подлинности инициатора (логин/пароль или токен аутентификации);";

Пункт 10 дополнить частью второй следующего содержания:

"При получении согласия у субъекта способами, запрос/ответ средствами инициатора и (или) оператора и запрос/ответ средствами инициатора в рамках оказания проактивной услуги, инициатор и (или) оператор формирует запрос на доступ к персональным данным с отображением информации к каким персональным данным будет предоставлен доступ и на какой период.";

пункт 13 дополнить подпунктом 8) следующего содержания:

"8) Уникальный идентификатор токена безопасности сформированный государственным сервисом;";

пункт 14 дополнить подпунктом 6) следующего содержания:

"6) Проверка токена безопасности в государственном сервисе на предмет создания в государственном сервисе и отзыв со стороны субъекта.";

дополнить параграфом 5 следующего содержания:

"Параграф 5. Процесс отзыва токена безопасности

16. Запрос на отзыв токена безопасности формируется субъектом посредством систем "электронного правительства";

17. На основании запроса на отзыв токена безопасности государственный сервис формирует заявку на отзыв токена безопасности к инициатору и (или) оператору для рассмотрения;

18. Инициатор и (или) оператор рассматривает заявку на отзыв токена безопасности в течение 15 рабочих дней. Субъект или его законный представитель не может отозвать

согласие на сбор, обработку персональных данных в случаях, если это противоречит законам Республики Казахстан, либо при наличии неисполненного обязательства согласно статьи 8 Закона "О персональных данных и их защите";

19. При условии положительного рассмотрения, инициатором и (или) оператором, заявки на отзыв токена безопасности, государственный сервис переводит токен безопасности в статус "не активный";

20. При условии отрицательного рассмотрения, инициатором и (или) оператором, заявки на отзыв токена безопасности, инициатор и (или) оператор должны указать причины и основание отказа в отзыве токена безопасности;

В основании для отказа в отзыве токена безопасности указывается ссылка на нормативный документ, договор (номер, дата, наименование) или иное неисполненное обязательство;

21. При условии отсутствия рассмотрения, инициатором и (или) оператором, заявки на отзыв токена безопасности, в течение 15 рабочих дней, государственный сервис переводит токен безопасности в статус "не активный".

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательством порядке 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 после его официального опубликования;

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 *Ж. Мадиев*
Республики Казахстан