



Об утверждении Правил функционирования государственного сервиса контроля доступа к персональным данным

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2022 года № 144/НК. Зарегистрирован в Министерстве юстиции Республики Казахстан 7 мая 2022 года № 27963

В соответствии с подпунктом 7-2) пункта 1 статьи 27-1 Закона Республики Казахстан "О персональных данных и их защите" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила функционирования государственного сервиса контроля доступа к персональным данным.

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
Министра цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 29 апреля 2022 года № 144/НК

Правила функционирования государственного сервиса контроля доступа к персональным данным

Глава 1. Общие положения

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) и определяют порядок функционирования государственного сервиса контроля доступа к персональным данным.

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

3) 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;

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

5) 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;

6) 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;

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

8) 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;

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

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

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

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

Глава 2. Порядок функционирования государственного сервиса контроля доступа к персональным данным

Параграф 1. Процесс функционирования государственного сервиса контроля доступа к персональным данным

3. Функционирование государственного сервиса контроля доступа к персональным данным осуществляется при автоматизации следующих процессов:

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

2) предоставление субъектом или его законным представителем согласия (отказа) на сбор и (или) обработку персональных данных, содержащихся в объектах информатизации государственных органов и (или) государственных юридических лиц;

3) отзыв субъектом или его законным представителем согласия на сбор и (или) обработку персональных данных, содержащихся в объектах информатизации государственных органов и (или) государственных юридических лиц;

4) уведомление субъекта о действиях с его персональными данными, содержащимися в объектах информатизации государственных органов и (или) государственных юридических лиц (доступ, просмотр, изменение, дополнение, передача, блокирование, уничтожение);

5) представление субъекту сведений о собственниках и (или) операторах, имеющих согласие на сбор и (или) обработку его персональных данных, содержащихся в объектах информатизации государственных органов и (или) государственных юридических лиц.

4. Процесс получения доступа к персональным данным осуществляется двумя 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 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);

5. Процесс получения доступа к персональным данным через SMS-шлюз Единого контакт-центра "1414" доступен инициаторам и (или) операторам, состоит из:

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

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

3) 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 через SMS-шлюз Единого контакт-центра "1414".

Государственный сервис проверяет наличие ответа от субъекта в SMS-шлюзе Единого контакт-центра "1414";

4) после получения ответа от государственного сервиса статуса "Ожидание ответа от субъекта", инициатор и (или) оператор отправляет повторный запрос с параметрами, соответствующими первому запросу;

5) формирования государственным сервисом токена безопасности при наличии положительного ответа от субъекта;

6) отправки токена безопасности государственным сервисом при повторном запросе доступа к персональным данным инициатором и (или) оператором и при наличии положительного согласия на сбор и (или) обработку персональных данных;

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

8) проверка собственником данных токена безопасности на соответствие запросу и сроку действия;

9) обработка запроса и отправление ответа собственником инициатору и (или) оператору.

6. Процесс получения доступа к персональным данным посредством запроса/ответа средствами инициатора и (или) оператора, не являющимся государственным органом и (или) государственным юридическим лицом, информационные системы которых соответствуют единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденным постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее - Единые требования), и имеющих акт испытаний на соответствие требованиям информационной безопасности, выданный уполномоченным государственным органом в соответствии с подпунктом 11-1) статьи 7-1 Закона Республики Казахстан "Об информатизации", состоит из:

1) получения инициатором и (или) оператором согласия у субъекта на доступ к его персональным данным следующими способами:

системы биометрии;

электронные цифровые подписи;

одноразовые пароли (ОТР);

система Digital ID;

бумажные носители информации.

2) отправки инициатором и (или) оператором запроса на доступ к персональным данным к государственному сервису с открытым ключом электронно-цифровой подписи (далее – ЭЦП) в токене верификации;

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

4) проверки государственным сервисом подписи токена верификации на соответствие, представленного ЭЦП;

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

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

7) проверки государственным сервисом даты формирования токена верификации;

8) формирования государственным сервисом токена безопасности при прохождении всех проверок токена верификации;

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

10) проверки собственником токена безопасности на соответствие запросу и сроку действия;

11) обработки запроса и отправление ответа собственником инициатору и (или) оператору.

Параграф 2. Процесс отправки запроса на доступ к персональным данным

7. Запрос на доступ к персональным данным направляется в формате согласно Единым требованиям и содержит следующие данные:

- 1) индивидуальный идентификационный номер субъекта;
- 2) наименование организации, инициатора и (или) оператора;
- 3) бизнес-идентификационный номер или индивидуальный идентификационный номер инициатора и (или) оператора;
- 4) идентификационные данные работника (фамилия имя отчество, учетная запись, индивидуальный идентификационный номер) инициатора и (или) оператора или при запросе на доступ к персональным данным без участия работника инициатора и (или) оператора указывается наименование организации или наименование информационной системы;
- 5) наименование организации собственника, при запросе информации у одного собственника;
- 6) наименование услуги в рамках которой осуществляется запрос на доступ к персональным данным;
- 7) список идентификаторов сервисов "ServiceID" ШЭП;
- 8) время, в течение которого действует токен безопасности при получении персональных данных и (или) государственных услугах (в миллисекундах);
- 9) признак способа отправки запроса и получения ответа от субъекта;
- 10) токен верификации указывается при выборе запрос/ответа средствами инициатора и (или) оператора.

8. Ответ по запросу на доступ к персональным данным субъектов заполняется в допустимом формате для взаимодействия через ШЭП.

9. Ответ по запросу на доступ субъектов, при положительном ответе содержит следующие данные:

- 1) "Доступ предоставлен", в соответствии запроса на доступ к персональным данным, возвращаемым государственным сервисом согласно приложению 1 к настоящим Правилам (далее – статус);
- 2) открытый ключ ЭЦП организации владельца государственного сервиса, необходимый для проверки достоверности токена безопасности;
- 3) токен безопасности.

10. Ответ по запросу на доступ к персональным данным, может принимать статус указанных в пунктах 2, 3, 4, 5, 6, 7, 8 согласно приложению 1 к настоящим Правилам.

Параграф 3. Процесс формирования токена безопасности

11. Токен безопасности используется для идентификации его владельца, который состоит из заголовка (header), полезной информации (payload) и подписан ЭЦП организации владельца государственного сервиса.

12. Заголовок токена безопасности содержит тип токена и алгоритм шифрования.

13. Полезная информация токена безопасности контроля доступа к персональным данным имеет общий вид согласно приложению 2 к настоящим Правилам и содержит:

1) индивидуальный идентификационный номер субъекта;

2) перечень кодовых наименований сервисов, в которых запрашиваются персональные данные;

3) дата и время получения положительного ответа от субъекта посредством SMS-сообщения через SMS-шлюз Единого контакт-центра "1414" в формате ISO 8601;

4) дата и время окончания действия токена безопасности, представляет собой сумму даты и времени получения положительного ответа от субъекта посредством SMS-сообщения через SMS-шлюз Единого контакт-центра "1414" и времени действия токена безопасности в формате ISO 8601;

5) бизнес идентификационный номер или индивидуальный идентификационный номер инициатора и (или) оператора;

6) дата и время получения положительного ответа от субъекта посредством SMS-сообщения через SMS-шлюз Единого контакт-центра "1414" в формате Unix Time Stamp;

7) дата и время окончания действия токена безопасности представляют собой сумму даты и времени получения положительного ответа от субъекта посредством SMS-сообщения через SMS-шлюз Единого контакт-центра "1414" и времени действия токена безопасности в формате Unix Time Stamp.

Параграф 4. Процесс проверки токена безопасности

14. При получении запроса на доступ к персональным данным, собственник извлекает из токена безопасности полезную информацию, используя открытый ключ ЭЦП, приложенную к запросу на доступ к персональным данным, и проверяет ее по следующим параметрам:

1) соответствие индивидуального идентификационного номера в запросе на доступ к персональным данным и токене безопасности;

2) наличие кодового наименования сервиса собственника в перечне кодовых наименований сервисов;

3) дата и время получения запроса на доступ к персональным данным не менее даты и времени получения положительного ответа от субъекта при запросе/ответе через Единый контакт-центр "1414" или даты и времени формирования токена при запросе/ответе средствами инициатора и/или оператора;

4) дата и время получения запроса на доступ к персональным данным не более даты и времени окончания действия токена безопасности;

5) проверка открытого ключа ЭЦП, приложенной к запросу на доступ к персональным данным.

15. При несоответствии одного из параметров, собственник отклоняет запрос на доступ к персональным данным.

Приложение 1
к Правилам функционирования
государственного сервиса
контроля доступа
к персональным данным
Министра цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 29 апреля 2022 года № 144/НК

Статус запроса на доступ к персональным данным, возвращаемые государственным сервисом

	Кодовое наименование	Статус	Описание
1	VALID	Доступ предоставлен	Доступ к персональным данным предоставлен субъектом персональных данных. Токен безопасности и открытая часть электронной цифровой подписи прилагаются в ответе
2	INVALID	В доступе отказано	В доступе к персональным данным отказано субъектом персональных данных
3	PENDING	Ожидание	Ожидание ответа от субъекта персональных данных
4	TIMEOUT	Время ожидания превышено	Время ожидания ответа субъекта персональных данных истекло
5	NOT_FOUND	Не найден в базе мобильных граждан	По указанному в запросе на доступ персональным данным индивидуальному идентификационному номеру отсутствует абонентский номер сети сотовой связи в БМГ

6	ERROR	Ошибка отправки (Запрос/ответ через "1414")	При отправке запроса на абонентский номер сети сотовой связи субъекта персональных данных, указанного в БМГ, возникла ошибка
7	ERROR_MCDB_SERVICE	Ошибка обращения к БМГ	Возникла ошибка при отправке запроса и (или) получения ответа БМГ
8	ERROR_MGOV_SMS_GW	Ошибка обращения к SMS-шлюзу Единого контакт центра "1414"	Возникла ошибка при отправке запроса для отправки SMS-сообщения в SMS-шлюз Единого контакт центра "1414".
9	ERROR_TV_NOTFOUND	Ошибка отправки (Запрос/ответ средствами инициатора и/или оператора)	Токен верификации не найден.
10	ERROR_TV_INVALID	Ошибка отправки (Запрос/ответ средствами инициатора и/или оператора)	Токен верификации не прошел проверку подписи.
11	ERROR_TV_BIN_NOTMATCH	Ошибка отправки (Запрос/ответ средствами инициатора и/или оператора)	Бизнес-идентификационный номер в токене верификации организации не соответствует Бизнес-идентификационный номер в запросе.
12	ERROR_TV_NOTINLIST	Ошибка отправки (Запрос/ответ средствами инициатора и/или оператора)	Способ получения доступа к персональным данным не соответствует значению из списка (Bio/Ds/Otp/DID/PC).
13	ERROR_TV_MOREDATE	Ошибка отправки (Запрос/ответ средствами инициатора и/или оператора)	Дата формирования токена верификации больше текущей даты.

Приложение 2
к Правилам функционирования
государственного сервиса
контроля доступа
к персональным данным
Министра цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 29 апреля 2022 года № 144/НК

Полезная информация токена безопасности контроля доступа к персональным данным

Кодовое наименование	Описание
uin	Индивидуальный идентификационный номер субъекта персональных данных
sid	Перечень кодовых наименований сервисов, в которых запрашиваются персональные данные
dts	Дата и время получения положительного ответа от субъекта персональных данных через SMS в формате ISO 8601 (данное условие применяется к схеме запроса посредством SMS-шлюза Единого контакт центра "1414").
dte	Дата и время окончания действия токена безопасности представляют собой сумму даты и время получения положительного ответа от субъекта персональных данных через SMS и времени действия токена безопасности в формате ISO 8601 (данное условие проверки применяется к схеме запроса посредством SMS-шлюза Единого контакт центра "1414").
binc	Бизнес идентификационный номер или индивидуальный идентификационный номер, инициирующий запрос персональных данных – Инициатором
iat	Дата и время получения положительного ответа от субъекта персональных данных через SMS в формате Unix Time Stamp
exp	Дата и время окончания действия токена безопасности, представляют собой дату и время получения положительного ответа от субъекта персональных данных через SMS и времени действия токена безопасности в формате Unix Time Stamp