Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

Утвърдена със Заповед № ДАЕУ-7420/28.04.2021 г.

М Е Т О Д И К А

за определяне от лицата по чл. 1, ал. 1 и 2 от Закона за електронното управление на средствата за електронна идентификация, които се използват при заявяване на електронни административни услуги и тяхното ниво на осигуреност

Глава Първа

Общи положения

Чл. 1. (1) Настоящата методика има за цел да подпомогне лицата по чл. 1, ал. 1 и 2 от Закона за електронното управление (ЗЕУ) в процеса по определяне на:

1. нивото на осигуреност на предоставяните електронни административни услуги (ЕАУ);
2. средствата за електронната идентификация, с които могат да се заявяват услугите по т. 1, както и нивото на осигуреност на тези средства.

(2) В зависимост от естеството на ЕАУ, процеса по предоставянето ѝ и риска от злоупотреба, услугата има определена степен на надеждност, изисква средството за електронна идентификация и съответстващото му ниво на осигуреност.

Чл. 2. Предмет на методиката са:

1. нормативно установените средства за електронна идентификация;
2. нивата на осигуреност на средствата за електронна идентификация;
3. критерии за оценка на риска за дадена ЕАУ;
4. метода за избор на подходящо средство за електронна идентификация с ниво на осигуреност, съответстващо на предоставяната ЕАУ, базиран на критериите по т. 3;

Чл. 3. По смисъла на тази методика:

1. „средство за електронна идентификация“ е материална и/или нематериална единица, която съдържа данни за идентификация на лица, която се използва за удостоверяване на автентичност за електронна услуга;

2. „данни за идентификация на лица“ са набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице.

3. „ниво на осигуреност на средството за електронна идентификация“ - характеризира степента на надеждност на това средство при установяване на самоличността на дадено лице, като по този начин се гарантира, че лицето, претендиращо, че има определена самоличност, действително е лицето, на което е приписана тази самоличност.

4. „доверяваща се страна“ означава физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга (съгласно чл. 3, пар. 6 от Регламент (ЕС) № 910/2014)

5. „чувствителни данни“ са специални категории лични данни, подлежащи на специфични условия на обработване, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравословното състояние или сексуалния живот и сексуалната ориентация на лицето (по смисъла на чл. 51, ал. 1 от Закона за защита на личните данни).

Глава Втора

Нормативно установени средства за електронна идентификация. Нива на осигуреност на средствата за електронна идентификация

Нормативно установени средства за електронна идентификация и техните нива на осигуреност

Чл. 4. На основание чл. 5, ал. 2 от ЗЕУ при заявяването на ЕАУ, която изисква идентификация на потребителя на услугата (физическо или юридическо лице), административните органи са длъжни да осигурят възможност на потребителя да се идентифицира чрез нормативно установено средство за електронна идентификация.

Чл. 5. Нормативно определените средства за електронна идентификация са:

1. електронен идентификатор, издаден по реда на Закона за електронната идентификация (ЗЕИ) - ще се прилага след въвеждане в продукционен режим на националната схема за електронна идентификация;

2. квалифициран електронен подпис (КЕП), в т.ч. облачен/мобилен квалифициран електронен подпис - прилага се в срок до една година след въвеждането в продукционен режим на националната схема за електронна идентификация;

3. персонален идентификационен код (ПИК), издаван от Националния осигурителен институт (НОИ) - прилага се в срок до три години след въвеждането в продукционен режим на националната схема за електронна идентификация;

4. персонален идентификационен код, издаван от Националната агенция за приходите (НАП) - прилага се в срок до три години след въвеждането в продукционен режим на националната схема за електронна идентификация;

5. уникален код за достъп (УКД), издаван от Националната здравноосигурителна каса (НЗОК) - прилага се в срок до три години след въвеждането в продукционен режим на националната схема за електронна идентификация;

6. други средства за електронна идентификация, издавани и поддържани от административните органи - могат да бъдат определени с решение на Министерския съвет.

Нива на осигуреност на средствата за електронна идентификация

Чл. 6. (1) Нивата на осигуреност на средствата за електронна идентификация са „ниско“, „значително“ и „високо“ и се определят в съответствие с чл. 8 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО, наричан по-нататък "Регламент (ЕС) № 910/2014", и с техническите спецификации, стандарти и процедури, включително технически проверки, подробно описани в Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 година за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно чл. 8, параграф 3 от Регламент (ЕС) № 910/2014.

(2) Ниво на осигуреност „ниско“ се отнася за средство за електронна идентификация, което предоставя ограничена степен на надеждност на претендираната или заявената самоличност на дадено лице.

(3) Ниво на осигуреност „значително“ се отнася за средство за електронна идентификация, което предоставя значителна степен на надеждност на претендираната или заявената самоличност на дадено лице.

(4) Ниво на осигуреност „високо“ се отнася за средство за електронна идентификация, което предоставя по-висока степен на надеждност на претендираната или заявената самоличност на дадено лице, отколкото средствата за електронна идентификация с ниво на осигуреност „значително“.

Чл. 7. (1) Когато средството за електронна идентификация отговаря на изискванията за по-високо ниво на осигуреност, се счита, че то изпълнява равностойно изискванията за всички по-ниски нива на осигуреност.

(2) Когато за заявяване на ЕАУ се изисква идентификация със средство с „ниско“ или „значително“ ниво на осигуреност, услугата може да бъде заявена и с всяко средство с по-високо ниво на осигуреност, съответно „значително“ или „високо“.

(3) Когато за заявяване на ЕАУ се изисква идентификация със средство със „значително“ ниво на осигуреност, услугата може да бъде заявена и с всяко средство с по-ниско ниво на осигуреност (ПИК на НАП, ПИК на НОИ, УКД на НЗОК), за което е въведена допълнителна еднократна парола (втори фактор) за автентикация, генерирана от модула за

двуфакторна автентикация, част от хоризонталната система за еАвтентикация, изградена и поддържана от Държавна агенция за електронно управление (ДАЕУ). Еднократната парола може да бъде кратко текстово съобщение (sms); еднократна хипервръзка на електронна поща или еднократна, базирана на време парола (TOTP). Достъп до ЕАУ се получава само след успешното представяне на втория фактор към хоризонталната система за еАвтентикация.

Чл. 8. Нивото на осигуреност на средствата за електронна идентификация се определя въз основа на надеждността и качеството на следните елементи:

1. вписване:
а) процедура за заявяване на средство за електронна идентификация и регистриране;
б) процедура за доказване и проверка на самоличността на физически и юридически лица, подаващи искане за издаване на средство за електронна идентификация;

2. управление на средствата за електронна идентификация:
а) характеристики и структура на средствата за електронна идентификация;
б) издаване, предоставяне и активиране на средство за електронна идентификация ;
в) временно спиране на действието, отнемане и повторно активиране;
г) подновяване и замяна;

3. удостоверяване на автентичност:
а) механизъм за удостоверяване на автентичност, чрез който потребителят на ЕАУ използва своето средство за електронна идентификация, за да потвърди самоличността си пред доверяваща се страна;

4. управление и организация:
а) управление на риска;
б) публикувани известия и информация за потребителите;
в) управление на информационната сигурност;
г) водене на отчетност;
д) съоръжения и персонал;
е) технически проверки;
ж) спазване и одит.

Глава Трета

Метод за определяне на нивото на осигуреност на средствата за електронна идентификация при заявяване и предоставяне на ЕАУ

Чл. 9. При определяне на средството за електронна идентификация, което ще се използва при заявяване на електронни административни услуги, е необходимо да се имат предвид следните критерии:

1. обработват ли се лични данни при предоставяне на услугата и по-специално:

а) вид данни и тяхното естество;

б) обработва ли се ЕГН/ЛНЧ или друг аналогичен идентификатор;

в) обработват ли се особено чувствителни данни;

д) какви са характеристиките на самия процес по обработването на данните;

е) какви са рисковете за лицето, застрашено от злоупотреба с данни (необходимо е да се познават последиците от всеки възможен вид загуба или неправомерно обработване на данни);

2. при оценяване естеството на личните данни са важни следните въпроси:

а) личната информация, която се предоставя и използва - за религия, вяра, раса, политическа принадлежност, здравословно състояние, сексуалност, членство в професионална организация, данни за съдебни присъди и информация за наложени забрани в резултат на противоправно поведение;

б) информация за финансово или икономическо състояние на лицето;

в) информация, която би могла да доведе до стигматизация или изолация на лицето, напр. данни за професионални постижения или за проблемни взаимоотношения;

г) информация за хора в неравностойно положение;

д) информация, с която би могло да се злоупотреби с цел кражба на идентичност, напр. биометрични данни, копия на документи за самоличност и ЕГН/ЛНЧ;

3. при оценяване на рисковете (естеството) на обработването на данните се разглеждат следните критерии:

а) обработват ли се големи обеми от лични данни на потребителя на електронни административни услуги;

б) какви са целите на обработването на данните - с колкото по-дълготрайни последици са решенията, които се вземат въз основа на обработваните лични данни, толкова по-голямо би било въздействието при загуба или неправомерно обработване;

в) степента, в която е възможна злоупотреба с информацията - преценява се основно възможността за кражба на самоличност.

4. какви са правните последици от предоставената услуга - използването на услугата може да има правни последици, ако за нея има правно основание и тя води до правни действия (директни или индиректни);

5. услугата предизвиква ли промени в данни (създаване, изменение или заличаване), съдържащи се в ключови регистри, например информация от регистър „ГРАО“;

6. какъв е икономическият интерес от услугата:

а) възможно ли е да се стигне до икономически щети (загуба на пари или икономическо положение; подвеждане под отговорност;

б) достъп на неоторизирани лица до конкурентно чувствителна информация или изтичане на ценово чувствителна информация) при грешна идентификация, кражба на самоличност или незаконосъобразно или неправилно обработване на данни;

в) икономическите щети могат да са за отделния гражданин или фирма или на системно ниво (за всички лица или за големи групи субекти);

7. какъв е публичният интерес от услугата - публичност и политически вълнения, от една страна, и социални сътресения, от друга страна:

а) тук се има предвид срив на общественото доверие в предоставяната услуга и съответната организация;

б) как могат да се решат проблемите (от една организация; сътресенията изискват координирани действия на няколко организации, както публични, така и частни; извънредни положения, които могат да изискат вземането на мерки извън обичайните правни и финансови рамки);

8. колко ЕАУ се предлагат от съответния административен орган и какви са техните потребители - граждани, фирми или и двете; включва ли предлагането на услугата трафик между различни информационни системи с искане за получаване на информация, респ. нейното получаване; гражданите действат от свое име или има възможност и за упълномощаване на лица, които да действат от тяхно име и за тяхна сметка;

9. наличие на внедрена система за управление на информационната сигурност и защита на личните данни; налице ли е внедрен и актуален план за IT сигурност;

10. автентикация на потребителя при заявяване и предоставяне на услугата - същият автентикира ли се преди да му се разреши достъп до услугата и неговата идентичност използва ли се в процеса по предоставяне на услугата; изискват ли се от потребителя допълнителни доказателства за потвърждаване на неговата идентичност в хода на предоставяне на услугата;

11. услугата включва ли издаване на решение от административен орган, за което следва да бъдат уведомени заинтересованите лица и което може да се извършва по канали, различни от тези, по които се предоставя услугата.

Чл. 10. (1) Всеки административен орган следва да направи преценка кои от критериите по чл. 9 са приложими по отношение на предоставяните от него ЕАУ. В Приложение № 1 е онагледено как дадените критерии водят до избор на средство за електронна идентификация със съответното ниво на осигуреност.

(2) Чрез предложения в Приложение №1 метод административните органи могат, в зависимост от конкретните особености на предоставяната от тях ЕАУ, на базата на опростен анализ на риска да определят вида средство за електронна идентификация, съобразно нивото му на осигуреност.

(3) Рисковете се преценяват конкретно за всяка услуга, като се вземат предвид и конкретните намаляващи и/или увеличаващи риска обстоятелства.

(4) При наличие на множество увеличаващи риска обстоятелства, може да се наложи прилагане на пълна оценка на риска (Приложение № 2) по следната формула:

оценка на въздействие x оценка на вероятност = оценка на риска

(**5**) Средствата за електронна идентификация, с които се заявяват и получат ЕАУ, следва да са с едно и също ниво на осигуреност.

Чл. 11. (1) Нивата на осигуреност на средствата за електронна идентификация съответстват на нивата на осигуреност на услугите, които се определят на базата на критериите по чл. 9 и съгласно Приложение 1.

(2) Средствата за електронна идентификация и тяхното нивото на осигуреност, както и нивото на осигуреност на ЕАУ задължително се посочват и в случаите, когато административен орган, подава заявление за присъединяване към хоризонталната система за електронна автентикация, поддържана от ДАЕУ.

Чл. 12. Отговорността за определяне на необходимите нива на осигуреност и риск за всяка услуга е на отделния доставчик на услуги (административен орган), който отговаря за данните, които се достъпват чрез определеното ниво на осигуреност.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата методика се издава на основание чл. 7в, т. 1, б. “в“ във връзка с чл. 5 от ЗЕУ.

Приложение № 1

Метод за определяне на нивото на осигуреност на средствата за електронна идентификация на базата на ключови критерии за опростена оценка на риска при предоставяните ЕАУ

Критерии по отношение на ЕАУ	**Ниво на осигуреност на средствата за електронна идентификация**
➢ Не се обработват лични данни; ➢ Не се използва ЕГН; ➢ Няма правни последици; ➢ Не настъпват изменения в ключови регистри; ➢ Няма икономически интерес; ➢ Няма публичен интерес.	не се изисква ниво на осигуреност
➢ Обработват се лични данни с незначителен риск; ➢ Обработва се ЕГН; ➢ Има косвени правни последици; ➢ Изменения само на нерискови данни от ключови регистри; ➢ Нисък икономически интерес; ➢ Нисък публичен интерес.	ниско
➢ Лични данни с висок риск; (специални лични данни, като напр. финансова, имуществена информация) ➢ Утежняващ фактор за личните данни от предходното ниво на осигуреност, свързан с естеството на обработката им; (напр. обработка на голям обем лични данни - медицинско досие; когато информацията благоприятства злоупотреба - кражба на идентичност; обработката е с цел издаване на широкообхватно решение, което повишава риска от загуба, злоупотреба с данни) ➢ ЕГН се обработва заедно с допълнителни лични данни; ➢ Директни правни последици; ➢ Предоставят се или се изменят данни от ключови регистри, които не попадат в категорията „високо" ниво на осигуреност; ➢ Умерен икономически интерес; ➢ Умерен публичен интерес;	значително
➢ Лични данни с най-висок риск; (информация от органите на наказателно преследване, от ДНК бази данни, информация, която е обект на специална, законова закрила, данни, които са обект на професионална тайна, като медицинска, здравна информация за пациент) ➢ Утежняващ фактор за личните данни от предходното ниво, свързан с естеството на обработката им; ➢ ЕГН се обработва заедно с допълнителни лични данни; ➢ Създаване, изменение или унищожаване на данни от ключови регистри; ➢ Значителен икономически интерес; ➢ Значителен публичен интерес.	високо

Приложение № 2

Примерен пълен анализ на риска

Етапи на анализ и оценка на риска:

- Да се идентифицират и анализират всички потенциални нежелани събития, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
- Да се оцени вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;
- Да се оцени въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки.

Оценка на въздействието

За всяка заплаха се оценява нейното въздействие - щетите (материални и нематериални), които дадена заплаха може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи: т. е. 1- незначителни, 2- значителни, 3- големи, 4- по-големи и 5- най-големи.

Оценка на вероятността

Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата.
За оценка на вероятността се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:
1 - вероятността от реализирането на заплахата е под 10 %;
2 - вероятността от реализиране на заплахата е от 10 % до 30 %;
3 - вероятността от реализиране на заплахата е от 30 % до 50 %;
4 - вероятността от реализиране на заплахата е от 50 % до 70 %;
5 - вероятността от реализиране на заплахата е над 70 %.

Оценка на риска

За получаване на оценката на риска се използва следната формула:

Оценка на въздействие* × *Оценка на вероятност* = *Оценка на риска

		вероятност				
		10 %	*30%*	*50 %*	*70 %*	*над 70 %*
въздействие	*1*	*ниско*	*ниско*	*ниско*	*ниско*	*значително*
	2	*ниско*	*ниско*	*значително*	*значително*	*значително*
	3	*ниско*	*значително*	*значително*	*значително*	*високо*
	4	*ниско*	*значително*	*значително*	*високо*	*високо*
	5	*значително*	*значително*	*високо*	*високо*	*високо*