ЗАКОН ЗА ЕЛЕКТРОНСКИ ДОКУМЕНТИ, ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА И ДОВЕРЛИВИ УСЛУГИ (*)

Редакциски пречистен текст[1]

I. ОПШТИ ОДРЕДБИ

Предмет

Член 1

(1) Со овој закон се уредува создавањето, складирањето и обработката на електронските документи, електронската идентификација и доверливите услуги.

(2) Со овој закон се уредува и употребата на електронските документи, електронскиот потпис и електронскиот печат и електронските доверливи услуги во управни и судски постапки.

(3) Предмет на уредување на овој закон се условите под кои се признаваат средствата за електронска идентификација издадени на физички и правни лица кои спаѓаат во рамки на регистрирана или признаена шема за електронска идентификација.

Цел

Член 2

(1) Целта на овој закон е обезбедување на безбедност на средствата за електронска идентификација и безбедност при обезбедување доверливи услуги.

(2) Цел на овој закон е уредување на електронските потписи, електронските печати, електронските временски жигови, електронските документи, услугите за електронска препорачана достава, услугите за проверка на автентичност на веб страници, зачувувањето на електронскиот потпис или печат и нивната валидација, електронските потврди на атрибути, средствата за создавање на електронски потпис, средствата за создавање на електронски печат и електронските записници, како и постапката на обезбедување на дигитален паричникот за електронски идентитет.

(3) Целта на овој закон е да се обезбедат услови за остварувањето на правото на физички и правни лица да учествуваат безбедно во дигиталното општество и да пристапуваат до електронски услуги обезбедени од јавниот или приватниот сектор.

Дефиниции

Член 3

(1) Одделни изрази употребени во овој закон, го имаат следново значење:

(*) Со овој закон се врши усогласување со Регулативата (ЕУ) 2024/1183 НА ЕВРОПСКИОТ ПАРЛАМЕНТ И НА СОВЕТОТ од 11 април 2024 година за изменување на Регулативата (ЕУ) бр. 910/2014 во однос на воспоставувањето на европската рамка за дигитален идентитет, CELEX бр. 32024R1183.

[1] Редакциски пречистениот текст на Законот за електронски документи, електронска идентификација и доверливи услуги ги опфаќа: основниот текст на Законот, објавен во "Службен весник на РСМ" бр.101/19, Законот за изменување и дополнување на Законот електронски документи, електронска идентификација и доверливи услуги, објавен во "Службен весник на РСМ" бр.275/19, Законот за изменување и дополнување на Законот електронски документи, електронска идентификација и доверливи услуги, објавен во "Службен весник на РСМ" бр.3/25 и Законот за изменување и дополнување на Законот електронски документи, електронска идентификација и доверливи услуги, објавен во "Службен весник на РСМ" бр.135/25, во кои е означено времето на нивното влегување во сила и примена.

1) формат на електронски податоци се податоци создадени во електронска форма, погодни за електронска обработка и пренос преку електронски комуникациски системи;

2) електронска трансакција е активност помеѓу две или повеќе страни, којашто се извршува по електронски пат;

3) електронски документ е секоја содржина складирана во електронска форма, особено текстуални или звучни, визуелни или аудио-визуелни записи;

4) производ е хардвер, софтвер или соодветните компоненти на хардвер или софтвер наменети да се користат при обезбедување на доверливи услуги и електронска идентификација;"

5) интероперабилност е способноста на два или повеќе системи или нивните компоненти за размена на податоци и олеснување на заедничката употреба на податоци и знаење;

6) јавен орган е државен орган, орган на државната управа, единица на локалната самоуправа, јавни претпријатија, установи, организации и правни лица на кои им се делегирани јавни овластувања во согласност со законодавството на Република Северна Македонија;

7) автентикација е електронски процес кој овозможува потврда на електронска идентификација на физичко или правно лице или кој овозможува потврдување на потеклото и интегритетот на податоците во електронска форма;

8) податоци за идентификација на лица се збир на податоци врз основа на кои единствено е можно да се идентификува правно или физичко лице или физичко лице или друго физичко лице кое го претставува физичкото лице или правното лице;

9) електронска идентификација е процес на користење на податоци за идентификација на лица во електронска форма кои на уникатен начин го претставуваат физичкото или правното лице, физичкото лице кое претставува друго физичко лице или правно лице;

10) средствата за електронска идентификација се материјални или нематеријални средства кои содржат податоци за идентификација на лица, а се користат за автентикација, а доколку е возможно и за автентикација при користење на офлајн електронски услуги;

11) издавач на средство за електронска идентификација е правно лице кое ги исполнува условите утврдени во овој закон за издавачи на средство за електронска идентификација;

12) шема за електронска идентификација е систем за електронска идентификација според кој средствата за електронска идентификација се издаваат на физички или правни лица или физичко лице кое претставува друго физичко лице или правно лице;

13) доверлива услуга е електронска услуга при електронски трансакции, која се состои од:

- создавање или валидација на сертификати за електронски потписи, сертификати за електронски печати, сертификати за електронски временски жигови, сертификати за автентичност на веб-страници, електронски потврди на атрибути или сертификати кои произлегуваат од обезбедување на други видови доверливи услуги,

- зачувување на електронски потписи, електронски печати, сертификати за електронски потписи или сертификати за електронски печати,

- создавање или валидација на електронски потписи или електронски печати,

- управување со средства за создавање на електронски потпис или печат од далечина,

- електронска препорачана достава,

- валидација на податоци или поврзани докази пренесени со користење на електронска препорачана достава,

- електронско складирање на електронски податоци и документи и

- запишување на електронски податоци во електронски записник;

Доверливите услуги може да бидат неквалификувани и квалификувани.

14) давател на доверлива услуга е правно лице кое обезбедува една или повеќе доверливи услуги;

15) засегната страна е физичко или правно лице кое има правен интерес од употреба на електронска идентификација, доверливи услуги или дигитален паричник за електронски идентитет;

16) квалификувана доверлива услуга е вид на доверлива услуга што ги исполнува условите утврдени со овој закон кои се однесуваат за квалификувана доверлива услуга;

17) давател на квалификувана доверлива услуга е давател на доверлива услуга кој обезбедува една или повеќе квалификувани доверливи услуги и чиј статус на давател на квалификувана доверлива услуга е доделен од страна на министерот за дигитална трансформација (во натамошниот текст: министерот) со регистрација во Регистарот на шеми за електронска идентификација и на доверливи услуги.

Давател на квалификувана доверлива услуга е правно лице на кое му се доделени јавни овластувања, согласно со одредбите од овој закон;

18) електронски потпис е збир на податоци во електронска форма кој е придружен кон или е логички поврзан со други податоци во електронска форма и кој потписникот го користи за потпишување;

19) електронски печат е збир на податоци во електронска форма кој е придружен кон или е логички поврзан со други податоци во електронска форма, со што се обезбедува сигурност на потеклото и интегритетот на придружените или поврзаните податоци;

20) податоци за изработка на електронски потпис се единствени податоци кои се користат од страна на потписникот за создавање на електронски потпис;

21) податоци за валидација се податоците кои се користат за валидација на електронски потпис или електронски печат;

22) сертификат за електронски потпис е електронска потврда која ги поврзува податоците за валидација на електронскиот потпис со физичко лице и која го потврдува најмалку името или псевдонимот на тоа лице;

23) сертификат за електронски печат е електронска потврда која ги поврзува податоците за валидација на електронскиот печат со правното лице и која го потврдува името на правното лице;

24) потписник е физичко лице кое создава електронски потпис;

25) создавач на електронски печат е правно лице кое создава електронски печат и истото во смисла на овој закон е определено и како запечатувач;

26) средство за создавање на електронски потпис или електронски печат е техничко средство, односно конфигуриран софтвер или хардвер, што се користи за создавање електронски потпис или електронски печат;

27) валидација е постапката за проверка и потврдување дека податоците во електронска форма се валидни доколку се создадени согласно одредбите од овој закон;

27-а) податоци за валидација се податоци кои се користат за валидација на електронски потпис или електронски печат;

28) напреден електронски потпис е електронски потпис кој ги исполнува условите утврдени со овој закон кои се однесуваат за напреден електронски потпис;

29) квалификуван електронски потпис е напреден електронски потпис кој е создаден од средство за изработка на квалификуван електронски потпис и кој се заснова на квалификуван сертификат за електронски потпис;

30) средства за создавање на квалификуван електронски потпис или печат се средства кои ги исполнуваат условите утврдени во овој закон, а кои се однесуваат на средства за создавање на квалификуван електронски потпис или печат;

31) квалификуван сертификат за електронски потпис е сертификат за електронски потпис издаден од давател на квалификувана доверлива услуга и кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за електронски потпис;

31-а) средства за создавање на квалификуван електронски потпис или печат од далечина се квалификувани средства кои се управувани од давател на квалификувана доверлива услуга, во име на потписникот или создавачот на печатот, согласно одредбите од овој закон;

32) напреден електронски печат е електронски печат кој ги исполнува условите утврдени со овој закон кои се однесуваат за напреден електронски печат;

33) квалификуван електронски печат значи напреден електронски печат кој е изработен од средство за изработка на квалификуван електронски печат и кој се заснова на квалификуван сертификат за електронски печат;

34) податоци за изработка на електронски печат се единствени податоци кои се користат од страна на создавачот на електронски печат со цел создавање на електронски печат;

35) квалификуван сертификат за електронски печат е сертификат за електронски печат издаден од давател на квалификувана доверлива услуга и ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за електронски печат;

36) сертификат за автентичност на веб страница е потврда што овозможува да се потврди автентичноста на дадена веб страница и ја поврзува веб страницата со физичкото или правното лице на кое му е издаден сертификатот за автентичност на веб страница;

37) квалификуван сертификат за автентичност на веб страница е сертификат за автентичност на веб страница издадена од давател на квалификувана доверлива услуга и кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за автентичност на веб страница;

38) електронски временски жиг е збир на податоци во електронска форма кој поврзува други податоци во електронска форма со конкретно време и претставува доказ дека поврзаните податоци постоеле во конкретниот момент;

39) квалификуван електронски временски жиг е електронски временски жиг кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван електронски временски жиг;

40) електронска препорачана достава е услуга која овозможува пренос на податоци помеѓу трети страни по електронски пат и обезбедува доказ во врска со преносот на податоците, вклучувајќи доказ за испраќање и примање на податоците, а притоа го заштитува преносот на истите од ризикот од загуба, кражба, оштетување или недозволени измени;

41) квалификувана електронска препорачана достава е услуга за електронска препорачана достава што ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификувана електронска препорачана достава;

42) конверзија е промена на формата или форматот на документот од една форма или формат во друга форма или формат, така што содржината на документот останува непроменета;

43) дигитализација е процес на конверзија на документ чијашто форма не е електронска во дигитализиран документ;

44) дигитализиран документ е електронски документ што е создаден со дигитализација на оригинални документи во писмена форма;

45) електронско складирање на документи е услуга која обезбедува прием, складирање, пронаоѓање и бришење на документи или податоци во електронска форма со цел да се обезбеди нивната тајност и читливост, како и да се зачува нивниот интегритет, доверливост и доказ за потекло во текот на целиот период на нивното чување;

46) квалификувано електронско складирање на документи е чување на електронски документи или податоци во електронска форма согласно условите утврдени во овој закон;

47) ознака за доверба на доверлива услуга е ознака којашто е јасно препознатлива и којашто јасно упатува дека доверливата услуга ја обезбедува конкретен давател на доверлива услуга;

48) ознака за доверба на квалификувана доверлива услуга е ознака којашто е јасно препознатлива и којашто јасно упатува дека квалификуваната доверлива услуга ја обезбедува конкретен давател на квалификувана доверлива услуга;

48-а) ознака за доверба на дигитален паричник за електронски идентитет е ознака којашто е јасно препознатлива и којашто јасно упатува дека дигиталниот паричникот за електронски идентитет е издаден согласно одредбите од овој закон;

49) тело за оценување на сообразноста е правно лице акредитирано да врши проценка на усогласеноста за исполнетост на условите кои се однесуваат на давател на квалификувана доверлива услуга и на квалификувани доверливи услуги кои истиот ги обезбедува, како и сертификација на дигитални паричници за електронски идентитет или на средства за електронска идентификација;

50) лабораторија за тестирање е правно лице акредитирано да врши проценка на усогласеност на средствата за издавање на електронска идентификација, електронски потписи или електронски печати со условите определени со овој закон;

51) дигитален паричник за електронски идентитет е средство за електронска идентификација кое му овозможува на корисникот безбедно да ги чува, да ги управува и да врши валидација на податоците за идентификација и валидација на електронски потврди на атрибути, заради достава на истите до засегнати страни или други корисници на дигитални паричници за електронски идентитет, како и да потпишува со средства за создавање на квалификуван потпис или да печатира со употреба на средства за создавање на квалификуван печат;

52) атрибут е карактеристика, квалитет, право или дозвола на физичко или правно лице или предмет;

53) електронска потврда на атрибути е потврда во електронска форма која овозможува атрибутите да бидат автентицирани;

54) квалификувана електронска потврда на атрибути е електронска потврда на атрибути која е издадена од квалификуван давател на доверливи услуги и која ги исполнува условите утврдени во овој закон;

55) електронска потврда на атрибути издадена од или во име на институција од јавниот сектор која е автентичен извор на атрибутот е електронска потврда на атрибути издадена од институција од јавниот сектор која е одговорна за автентичниот извор, согласно условите утврдени со овој закон;

56) автентичен извор е репозиториум или систем, за чие чување е надлежна институција од јавниот сектор, што содржи и обезбедува атрибути за физичко или правно лице или предмет и што се смета дека е основен извор на тие информации или е признаен како автентичен извор согласно закон;

57) силна автентикација на корисник означува автентикација којашто се заснова на употреба на најмалку два фактора за автентикација од различни категории на:

- фактор што се знае: нешто што само корисникот го знае,
- фактор што се поседува: нешто што само корисникот го поседува или
- фактор што е својствен: нешто што корисникот е,

кои фактори се независни, така што загрозувањето на еден фактор не ја загрозува веродостојноста на другиот фактор и автентикацијата е создадена на таков начин што ја заштитува доверливоста на податоците.

58) електронски записник е хронолошка низа на електронски записи, која го потврдува интегритетот на податоците кои ги содржи, како и точноста на хронолошкиот распоред на податоците;

59) квалификуван електронски записник е електронски записник којшто е обезбеден од страна на давател на квалификувана доверлива услуга и којшто ги исполнува условите определени со овој закон;

60) впарување на идентитет е процес со којшто податоците за идентификација на лицето или средствата за електронска идентификација се впаруваат или се поврзуваат со постоечка корисничка сметка што му припаѓа на истото лице;

61) запис на податоци се електронски податоци кои се зачувани со поврзани мета-податоци, коишто ја поддржуваат обработката на податоците;

62) офлајн режим е употреба на дигитални паричници за електронски идентитет заради интеракција помеѓу нивниот корисник и трета страна кои се наоѓаат на иста физичка локација и употребуваат технологии за непосредна близина, така што дигиталниот паричник за електронски идентитет не се користи за пристап до далечински системи до кои се пристапува преку електронски комуникациски мрежи;

63) интерфејс е заедничка врска која ја користат две или повеќе посебни компоненти на компјутерски систем за размена на информации;

64) веб-прелистувач е софтверска апликација која им овозможува на крајните корисници пристап и интеракција со веб-содржини хостирани на сервери кои се поврзани на мрежи, вклучувајќи самостојни веб-прелистувачи, како и веб-прелистувачи интегрирани или вградени во софтвер;

65) основни платформски услуги се следниве услуги:

(а) услуги за онлајн посредување;
(б)онлајн пребарувачи;
(в) онлајн услуги за социјално вмрежување;
(г) услуги на платформа за споделување видео;
(д) услуги за интерперсонални комуникации;
(ѓ) оперативни системи;
(е) веб-прелистувачи;
(ж) виртуелни асистенти;

(з) компјутерски услуги во облак;

(ѕ) услуги за рекламирање преку интернет, вклучително и какви било рекламни мрежи, размена на реклами и какви било други услуги за посредување во рекламирањето, обезбедени од правно лице кое обезбедува некоја од основните платформски услуги;

66) протокол е начин на комуникација со употреба на техничко-технолошки средства кој обезбедува пренос на документи, податоци и пораки кои произлегуваат од различни процеси и овозможува сигурен и безбеден пренос помеѓу различни системи и

67) репозиториум е локација за чување, управување и одржување на податоци, документи, софтвер, кодови или други содржини, која овозможува структурирано организирање, пребарување и пристап до содржината, со цел лесно споделување и повторна употреба на зачуваните содржини.

(2) Изразите што се употребуваат во овој закон чие значење не е дефинирано во ставот (1) на овој член, имаат значење утврдено со друг закон.

Примена на законот

Член 4

(1) Одредбите од овој закон се применуваат и за спречување на перење на пари, преку идентификување на корисникот на доверливите услуги, потврдување на неговиот идентитет врз основа на обработка на документи, податоци или информации добиени од сигурен и независен извор, вклучувајќи и средства за електронска идентификација, соодветни доверливи услуги.

(2) Одредбите од овој закон кои се однесуваат на доверливи услуги не се применуваат во рамки на затворен систем или систем наменет за ограничена група на учесници, чијашто употреба може да се утврди со договор или со внатрешен акт, а кој систем нема влијание врз трети лица или не предизвикува обврски за трети страни надвор од тој систем.

Обработка и заштита на лични податоци

Член 5

(1) Давателот на доверлива услуга при обработката на личните податоци до кои има пристап во текот на вршењето на дејноста постапува согласно со прописите од областа на заштитата на личните податоци.

(2) При извршување на електронска трансакција, корисникот може да употреби и псевдоним, доколку користењето на псевдонимот кој е употребен не е во спротивност со одредбите од друг закон.

Пристапност на лица со попреченост

Член 5-а

Средствата за електронска идентификација, доверливи услуги и дигитален паричник за електронски идентитет (во натамошниот текст: дигиталниот паричник) за крајните корисници треба да бидат пристапни на лица со попреченост, достапни на јасен и разбирлив јазик согласно Конвенцијата на

Обединетите нации за правата на лицата со попреченост, како и да бидат пристапни за стари лица и лица со ограничен пристап до дигитални технологии согласно закон.

II. ЕЛЕКТРОНСКИ ДОКУМЕНТ

Правно дејство на електронскиот документ

Член 6

(1) Електронскиот документ има иста правна и доказна сила како и писмената форма на документот, согласно со закон.

(2) Електронскиот документ не може да се оспори како доказ во управна или судска постапка, само затоа што е создаден во електронски облик.

(3) Кога со закон е утврдена писмена форма на документите или актите, електронскиот документ се смета за документ или акт во писмена форма.

Создавање на електронски документ

Член 7

(1) Електронски документ се создава со користење на една или повеќе од достапните и употребливи информатички и комуникациски технологии, освен ако со друг закон поинаку не е уредено.

(2) Електронскиот документ како архивски материјал се создава во форма која ги исполнува условите утврдени во овој закон, а е погодна за подготовка за сигурносно електронско складирање.

(3) Електронските документи содржат задолжителни елементи.

(4) Задолжителните елементи на електронските документи ги пропишува министерот со правилник.

Оригинал и копија

Член 8

(1) Секој умножен електронски примерок на конкретен електронски документ се смета за оригинал.

(2) Електронски документ создаден со дигитализација на изворниот документ чија првична форма не е електронска, се смета за копија на оригиналниот документ.

(3) Кога електронскиот документ е репродуциран во хартиена форма се смета за копија на оригиналниот документ.

Дигитализација на документи

Член 9

(1) Дигитализираниот документ ја има истата правна и доказна сила како оригиналниот документ, ако:

1) дигитализацијата на документот е извршена под надзор или од страна на:

- физичко лице или овластено лице на правно лице којшто го создал документот што е предмет на дигитализација или

- лица кои се овластени да ракуваат со документи во кои се содржани потписи, ракописи или записници, согласно со прописите од областа на архивското и канцелариското работење или

- лица кои се овластени со закон да го потврдат дигитализираниот документ и

2) идентичноста на дигитализираниот документ со оригиналниот документ е потврдена со квалификуван електронски печат или квалификуван електронски потпис на лицата од точка 1) на овој член или лицето на кое се пренесени надлежностите врз основа на кои е донесен документот.

Верификација на печатена форма на електронски документ

Член 10

(1) Електронскиот документ репродуциран на кој било печатен медиум ја има истата правна и доказна сила како оригиналниот електронски документ, доколку:

1) умножувањето на електронскиот документ е извршено под надзор или од страна на физичко лице или овластено лице на правно лице кое го создало документот и

2) печатењето на документот е извршено на начин што идентичноста на електронскиот документ со печатениот документ се потврдува со своерачен потпис на физичко лице или овластено лице на правно лице.

(2) По исклучок на ставот (1) на овој член, печатена форма на електронскиот документ издаден од јавен орган, не подлежи на процесот на верификација од ставот (1) на овој член.

(3) Секој јавен орган и/или приватно правно лице до кој се доставува печатена форма на електронскиот документ од ставот (2) на овој член, може да направи проверка на неговата валидност преку скенирање на кодот на долниот десен агол на печатената форма на електронскиот документ (QR-код), кој ја содржи локацијата каде што може да се добие оригиналот на електронскиот документ.

III. ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

1. Шеми за електронска идентификација

Услови кои треба да ги исполнуваат шемите за електронска идентификација

Член 11

Шемите за електронска идентификација ги исполнуваат следните услови:

1) да вклучат потврда за податоците за идентификација на лицата на кои им се издадени средства за електронска идентификација, кои на единствен начин го определуваат правното или физичкото лице;

2) да обезбедат сигурност дека издавачот на средството за електронската идентификација обезбедува идентификациски податоци во рамките на средствата за електронска идентификација што соодветствуваат на лицето на кое му е издадено средството за електронска идентификација;

3) да ги исполнуваат условите за нивото на сигурност во кој е класифицирана шемата за електронска идентификација, од членот 13 од овој закон.

Согласност за идентификација

Член 12

Постапката за издавање на електронска идентификација се поведува по претходно барање на физичко или правно лице кое е субјект на идентификација пред издавач на средства за електронска идентификација освен ако со закон поинаку не е уредено.

Нивоа на сигурност на шемите за електронска идентификација

Член 13

Шемите за електронска идентификација се класифицирани според нивото на сигурност на средствата за електронска идентификација кои се издадени во рамките на таа шема и тоа:

1) ниско ниво на сигурност обезбедува ограничен степен на сигурност на бараниот или потврдениот идентитет на лицето и се карактеризира со упатување кон соодветни технички спецификации, стандарди и постапки, вклучувајќи и технички проверки, чија цел е намалување на ризикот од злоупотреба или промена на идентитетот;

2) значително ниво на сигурност обезбедува значителен степен на сигурност на бараниот или потврдениот идентитет на лицето и се карактеризира со упатување кон соодветните технички спецификации, стандарди и постапки, вклучувајќи и технички проверки, чија цел е значително да се намали ризикот од злоупотреба или промена на идентитетот и

3) високо ниво на сигурност обезбедува повисок степен на сигурност на бараниот или потврдениот идентитет на лицето отколку средствата за електронска идентификација со ниво на сигурност „значително" и се карактеризира со упатување кон соодветни технички спецификации, стандарди и постапки, вклучувајќи и технички проверки, чија цел е спречување на злоупотреба или промена на идентитетот.

Регистар на даватели на доверливи услуги и на шеми за електронска идентификација

Член 14

(1) Давателот на доверлива услуга до Министерството за дигитална трансформација (во натамошниот текст: Министерството), доставува барање за регистрација во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација (во натамошниот текст: Регистарот), кој го води Министерството.

(2) Во Регистарот задолжително се регистрираат шемите за електронска идентификација кои ги употребуваат јавните органи.

(3) Во Регистарот по претходно поднесено барање од страна на јавниот орган или приватното правно лице може да се регистрираат и шеми за електронска идентификација кои се создадени од јавни органи и шеми кои се создадени од приватни правни лица.

(4) Шемите создадени од јавните органи се регистрираат во Регистарот врз основа на решение за регистрација донесено од страна на министерот, а по претходно поднесено барање за регистрација на шема од страна на јавниот орган.

(5) Шемите создадени од приватни правни лица задолжително треба да одговараат на високо ниво за сигурност за да бидат регистрирани во Регистарот.

(6) Регистарот од ставот (1) на овој член особено ги содржи следните информации за давателот на доверлива услуга:

- име на правното лице,
- информации за контакт како што се: адреса, телефонски број и електронска пошта,
- видот на услуги што ги обезбедува издавачот на шемата за електронска идентификација,
- средствата за електронска идентификација кои се користат во рамки на шемата и
- нивото на сигурност.

(7) Во Регистарот се регистрираат и давателите на квалификувана доверлива услуга.

(8) Давателите на доверливи услуги и шемите за електронска идентификација може да бидат избришани од Регистарот, доколку:

- престанат да ги исполнуваат условите определени со овој закон,
- не бидат отстранети отстапувањата од овој закон по претходно укажување за отстранување на недостатоци во рокот утврден во решението за отстранување на неправилности издадено согласно со овој закон или
- во други случаи определени со закон за бришење на правни лица од евиденција на надлежен орган.

(9) Министерот ја пропишува содржината и начинот на водење на Регистарот од ставот (1) на овој член, како и начинот на поднесување на барањето за регистрација, потребната документација како прилог кон барањето, образецот на барањето и начинот на објавување на податоците од Регистарот, во зависност од видот на доверливоста на услугата.

Употреба на шеми за електронска идентификација во електронска трговија и комуникација со јавен орган

Член 15

(1) За електронска идентификација на лицето кое води постапка пред јавен орган, задолжително се користи шема за електронска идентификација која е регистрирана во Регистарот од членот 14 од овој закон (во натамошниот текст: регистрирана шема за електронска идентификација).

(2) За електронска идентификација на лицето кое презема дејствија поврзани со активностите на приватниот сектор, вклучувајќи и електронска трговија, по сопствен избор може да користи регистрирана шема или шема за електронска идентификација која не е регистрирана во Регистарот од членот 14 од овој закон.

Одговорност за штета од употреба на регистрирани шеми за електронска идентификација

Член 16

(1) Издавачот на регистрирана шема за електронска идентификација е одговорен за штетата која може да настане поради тоа што шемата не ги исполнува условите од овој закон.

(2) Штетата настаната како последица на погрешно спроведената постапка за валидација е одговорност на странката што ја води постапката, ако штетата била предизвикана намерно или од небрежност.

(3) Товарот за докажување за настаната штета е на страна на лицето што истакнало побарување за надоместок на штета.

(4) Издавачот од ставот (1) на овој член е должен да биде осигуран од евентуална штета која може да ја предизвика.

(5) Најнискиот износ од осигурувањето од евентуалната штета предизвикана од издавачот ќе го пропишува министерот.

Барање за утврдување на исполнетост на услови за нивоа на сигурност на шеми

Член 17

(1) Барањето за утврдување на исполнетост на услови за нивоа на сигурност на шеми е прилог кон барањето за регистрација во Регистарот од членот 14 од овој закон.

(2) Барањето од ставот (1) на овој член ги содржи следните информации:

1) начинот на докажување и верификација на идентитетот на физичко или правно лице кое бара издавање на средство за електронска идентификација;

2) начинот на издавање на средствата за електронска идентификација;

3) механизмите за автентикација, преку кои физичко или правно лице, користејќи ги средствата за идентификација, го потврдува својот идентитет на засегната страна;

4) условите што треба да ги исполнат останатите учесници вклучени во постапката за издавање средства за електронска идентификација;

5) техничките и безбедносните карактеристики на средствата за електронска идентификација што се издаваат во рамки на шемата;

6) технички и организациски мерки кои ги исполнува издавачот на средства за електронска идентификација со цел да се обезбеди интероперабилност на шемите за електронска идентификација во согласност со националните и меѓународните стандарди во оваа област;

7) извештај за ниво на сигурност на шемата за електронска идентификација од тело за оценување на сообразноста и

8) податоци за издавачот на шемата за електронска идентификација.

Безбедносни услови што треба да ги исполнат издавачите на шемите за електронска идентификација

Член 18

(1) Издавачот на шемата за електронска идентификација е должен да ги преземе потребните технички, физички и организациски мерки за управување со ризиците кои би можеле да го загрозат обезбедувањето на овие услуги на сигурен и безбеден начин.

(2) Техничките, физички и организациски мерки треба да обезбедат нивото на безбедност да одговара на нивото на ризик и предвиденото ниво на сигурност на шемата за електронската идентификација, земајќи ги предвид најновите достапни технолошки решенија, а особено мерките за спречување на безбедносни инциденти и за ограничување на штетните ефекти од можните инциденти, како и за информирање на засегнатите страни за несакани ефекти од безбедносни инциденти.

(3) Процедурите и стандардите за исполнетост на техничките, физички и организациски мерки за сигурност на шеми за електронска идентификација ги пропишува министерот.

(4) Оценката на нивото на сигурност на шемата за електронска идентификација ја оценува телото за оценување на сообразноста кое е акредитирано да врши сертификација по стандарди, определени во подзаконскиот акт од ставот (3) на овој член.

2. Прекугранична соработка во областа на електронската идентификација

Интероперабилност на техничките системи

Член 19

(1) Министерството соработува со надлежни меѓународни институции за прашањата поврзани со прекугранична интероперабилност на шемите за електронска идентификација и презема мерки во рамките на својата надлежност со цел да се утврди највисокото ниво на интероперабилност на шемите за електронска идентификација на национално ниво, со цел нивна интеграција и интероперабилност во меѓународно признатите шеми за електронска идентификација.

(2) Министерството соработува со надлежни меѓународни институции за прашањата поврзани со прекугранична интероперабилност на дигиталниот паричник, со цел да се утврди највисокото ниво на интероперабилност на дигиталниот паричник на национално ниво, и негова интеграција и интероперабилност во регистрите на сертифицирани европски дигитални паричници за дигитален идентитет.

Регистрација на шеми за електронска идентификација издадени од странски правни лица

Член 20

(1) Министерството може да регистрира во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација и странски правни лица кои се регистрирани како даватели на доверливи услуги или како издавачи на шеми за електронска идентификација на ниво на Европската Унија или во земја членка на унијата.

(2) Министерството може да регистрира во Регистарот и шеми за електронска идентификација кои одговараат на високо ниво на сигурност, доколку таа шема се користи од страна на земја членка на Европската Унија.

(3) Министерството може да регистрира во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација и странски правни лица кои се регистрирани како даватели на доверливи услуги или како издавачи на шеми за електронска идентификација во друга држава која не е земја членка на Европската Унија, врз основа на претходно склучен договор со кој се утврдува реципроцитет на шемите за електронска идентификација или/и на давателите на доверливи услуги помеѓу Република Северна Македонија и државата во кое е регистрирано правното лице.

Прекугранично впарување на идентитет

Член 20-а

(1) Издавачите на шеми за електронска идентификација обезбедуваат технички и организациски мерки заради обезбедување на високо ниво на заштита на личните податоци што може да се користат за прекугранично впарување на идентитетот.

(2) Листа на стандарди и спецификации за техничките и организациските мерки од ставот (1) на овој член ја утврдува министерот.

Сертификација на шеми за електронска идентификација

Член 20-б

(1) Сертификацијата на шеми за електронска идентификација се врши со оцена на сообразност на шемите за електронска идентификација со барањата за сајбер безбедност утврдени во овој или друг закон, вклучително и усогласеноста со барања за сајбер безбедност во однос на нивоата на сигурност на шемите за електронска идентификација, ја вршат телата за оцена на сообразност согласно овој закон.

(2) Сертификацијата од ставот (1) на овој член се врши според шема за сертификација за сајбер безбедност на ниво на Европската Унија, доколку шемата за сертификација за сајбер безбедност обезбедува целосна или делумна оценка на усогласеност на шемата за електронската идентификација со барањата за сајбер безбедност согласно закон.

(3) Сертификацијата од ставот (1) на овој член важи пет години, под услов издавачот на шемата за електронска идентификација да врши проценка на ранливост на секои две години.

(4) Доколку при спроведување на проценката на ранливост е идентификувана ранливост и истата не е отстранета во рок од три месеци од нејзиното идентификување, издавачот на шемата за електронска идентификација се брише од регистарот од член 14 став (1) од овој закон.

(5) Издавачот на шема за електронска идентификација е должен да ја достави сертификацијата од ставот (1) на овој член и проценката на ранливост до Министерството најдоцна во рок од 15 дена од денот на нивното добивање, односно спроведување.

Пристап до карактеристики на хардвер и софтвер

Член 20-в

Издавачите на дигитални паричници од член 20-д став (1) алинеја 3 од овој закон и издавачите на средства за електронска идентификација кои дејствуваат за комерцијални или професионални цели и користат основни платформски услуги за издавање или обезбедување на дигитален паричник или средство за електронска идентификација на крајни корисници се сметаат се деловни корисници, при што:

а) лицата што обезбедуваат основни платформски услуги според единствениот европски пазар им овозможуваат ефективна интероперабилност преку обезбедување на пристап до оперативниот систем и карактеристиките на хардверот и софтверот и

б) интероперабилноста и пристапот од точката а) на овој став се овозможуваат без надомест и независно од тоа дали карактеристиките на хардверот или софтверот се дел од оперативниот систем, се достапни или се користат од страна на лицето што ги обезбедува платформските услуги.

Дигитален паричник за електронски идентитет

Член 20-г

(1) Физичките и правните лица може да ги користат електронските услуги кои ги обезбедуваат институциите од јавниот сектор или приватниот сектор со употреба на дигитални паричници.

(2) Дигиталните паричници овозможуваат безбеден, доверлив и непрекинат пристап до електронските услуги и на корисниците им обезбедува целосна контрола врз нивните податоци, согласно закон.

(3) Кога физичките лица го употребуваат дигиталниот паричник за користење на електронски услуги за лични, а не за трговски, деловни, занаетчиски или професионални цели, можат да потпишуваат со квалификуван електронски потпис без надомест.

(4) Започнувањето со употреба на дигиталните паричници од страна на корисниците се врши со употреба на регистрирана шема за електронска идентификација на високо ниво на сигурност.

(5) Валидноста на дигиталниот паричник престанува во следниве случаи:

(а) по изрично барање за престанок на валидноста на дигиталниот паричник, од корисникот до издавачот на дигиталниот паричник;

(б) кога безбедноста на дигиталниот паричник е загрозена или

(в) со смртта на корисникот како физичко лице или со престанок на правното лице.

(6) Престанокот на валидноста на дигиталниот паричник во случаите од ставот (5) на овој член, предизвикува правно дејство од денот на неговиот престанок, освен во случаите од член 20-к од овој закон во кои е утврдено повлекување од употреба на издаден паричник заради нарушување на неговата безбедност.

Издавање на дигитални паричници

Член 20-д

(1) Дигитален паричник се издава и се обезбедува од:

- Министерството,
- институција од јавниот сектор или приватно правно лице како национален издавач на дигитален паричник или
- приватно правно лице кое е регистрирано како издавач на дигитален паричник.

(2) Изворниот код на компонентите на софтверот на дигиталниот паричник е лиценциран со лиценца за отворен код.

(3) По исклучок од ставот (2) на овој член, во случаи кога се работа за деловна тајна на издавачот на дигитален паричник, загрозување на безбедноста на дигиталниот паричник, загрозување на националната безбедност, заштита на авторските права, донесена судска одлука и во други случаи утврдени со закон, одредени компоненти на софтверот на дигиталниот паричник кои не се инсталирани на корисничките уреди, нема бидат откриени.

(4) Издавачите на дигиталните паричници обезбедуваат техничко-технолошки средства и стандарди за валидација, со кои вршат проверка на:

- автентичноста и валидноста на дигиталните паричници кои ги издале и издаваат и

- потврда на корисниците за автентичноста и валидноста на засегнатите страни регистрирани во Регистарот на засегнати страни од член 20-ѕ од овој закон.

(5) Издавачите на дигитален паричник на своите корисници обезбедуваат техничка поддршка, која треба да ја добијат при издавање на дигиталниот паричник, вклучително и да пријават технички проблеми или какви било други прекини кои имаат негативно влијание врз употребата на дигиталниот паричник.

(6) Дигиталните паричници се обезбедуваат со употреба на регистрирана шема за електронска идентификација на високо ниво на сигурност.

(7) Издавачите на дигиталните паричници обезбедуваат техничка и интегрирана заштита на дигиталните паричници.

(8) Издавањето, користењето и престанокот на користење на дигиталниот паричник е бесплатно за сите физички лица.

(9) Начинот на издавање на дигиталниот паричник, начинот на обезбедување на техничка поддршка од ставот (5) на овој член и начинот на обезбедување на техничка и интегрирана заштита од ставот (7) на овој член, ги пропишува министерот.

(10) Начинот на определување на националниот издавач на дигитален пичник од став (1) алинеја 2 на овој член го пропишува министерот.

(11) Националниот издавач од став (1) алинеја 2 на овој член го определува Владата.

Функционалности на дигиталниот паричник

Член 20-ѓ

(1) Дигиталниот паричник ги обезбедува следниве функционалности:

(а) безбедно барање, добивање, избирање, комбинирање, складирање, бришење, споделување и презентирање на податоците за идентификација на лицето, вклучително и доколку е применливо, комбинирање на овие податоци со електронските потврди на атрибути, со истовремено обезбедување на можност за селективно откривање на податоци, да се потврди нивната автентичност на засегнати страни во онлајн и, каде што е соодветно, во офлајн режим, со цел корисникот да пристапи до електронски услуги, под единствена контрола на корисникот;

(б) генерирање на псевдоними и локално енкриптирано складирање во дигиталниот паричник;

(в) безбедна автентикација на дигиталниот паричник на друго лице, како и примање и споделување на податоци за идентификација и електронски потврди на атрибути на безбеден начин помеѓу два дигитални паричници;

(г) пристап до евиденција на сите трансакции извршени преку дигиталниот паричник преку контролна табла што му овозможува на корисникот:

- преглед на ажурирана листа на засегнати страни со кои корисникот воспоставил врска и, каде што е применливо, сите разменети податоци,

- лесно да побара бришење на личните податоци од страна на засегната страна согласно прописите за заштитата на личните податоци,

- лесно да пријави засегната страна до Агенцијата за заштита на личните податоци, кога се сомнева за незаконско или сомнително барање за податоци;

(д) потпишување со квалификуван електронски потпис или печатирање со квалификуван електронски печат;

(ѓ) преземање, до степен што е технички изводлив на податоците за корисникот, електронските потврди на атрибути и поставките за користење на дигиталниот паричник;

(е) овозможување на слободен пренос на лични податоци од страна на корисникот во дигиталниот паричник.

(2) Издавачите на дигитални паричници може да обезбедат дополнителни функционалности на дигиталниот паричник, вклучително и интероперабилност со регистрираните средства за електронска идентификација, доколку тие дополнителни функционалности не се во спротивност со функционалностите од ставот (1) на овој член, а се согласно закон.

Протоколи и интерфејси на дигитален паричник

Член 20-е

(1) За да може дигиталниот паричник да се користи треба да има интерфејс и да ги поддржува протоколите за:

- издавање на податоци за идентификација на лица, квалификувани и неквалификувани електронски потврди на атрибути или квалификувани и неквалификувани сертификати во дигитален паричник,

- засегнатите страни да побараат и да ги потврдат податоците за идентификација на лице и електронските потврди на атрибути,

- споделување и презентирање на податоци за идентификација на лица, електронски потврди на атрибути или на селективно откривање на поврзани податоци на засегнати страни, онлајн и, каде што е соодветно, во офлајн режим,

- корисникот да дозволи интеракција со дигитален паричник и да ја прикаже ознаката за доверба на дигитален паричник,

- безбедна регистрација на корисник со употреба на средства за електронска идентификација издадени во рамки на регистрирана шема за електронска идентификација на високо ниво на сигурност,

- интеракција помеѓу дигитални паричници на две лица со цел безбедно примање, потврдување и споделување податоци за идентификација на лице и електронски потврди на атрибути,

- автентикација и идентификување на засегнатите страни преку спроведување механизми за автентикација согласно овој закон,

- засегнатите страни да ја потврдат автентичноста и валидноста на дигиталниот паричник,

- барање од засегнатата страна да ги избрише лични податоци во согласност со прописите од областа на заштитата на личните податоци,

- пријавување на засегната страна до Агенцијата за заштита на личните податоци кога е примено незаконско или сомнително барање за податоци и

- создавање квалификувани електронски потписи или електронски печати преку употреба на средства за создавање на квалификувани електронски потписи или печати.

(2) Дигиталниот паричник не треба да доставува информации на давателите на услугата за електронска потврда за атрибути во врска со употребата на тие електронски потврди.

(3) Засегнатите страни кои имаат намера да овозможат употреба на дигиталниот паричник треба да бидат автентифицирани и идентификувани согласно овој закон за да може да се употребува дигиталниот паричник.

(4) Дигиталниот паричник треба да ги исполни условите кои се однесуваат на високо ниво на сигурност од член 13 од овој закон, а особено барањата за потврда и верификација на идентитет и употреба и автентикација на средства за електронска идентификација.

(5) Во случај на барање за електронска потврда на атрибути од страна на засегнатата страна или од друг корисник на дигиталниот паричник, корисникот на дигиталниот паричник се известува дека засегнатата страна или друг корисник на дигиталниот паричник имаат дозвола за пристап.

(6) Податоците за идентификација на корисникот кои се достапни преку шемата за електронска идентификација која се користи за дигиталниот паричник, јасно и точно го идентификуваат секое физичко или правно лице кое го користи дигиталниот паричник.

Користење на дигиталниот паричник и управување со податоците

Член 20-ж

(1) На корисниците на дигиталниот паричник им се обезбедува целосна контрола врз употребата на дигиталниот паричник, како и на податоците содржани во нивниот дигитален паричник.

(2) Издавачот на дигитален паричник не смее да собира информации за употребата на дигиталниот паричник кои не се неопходни за обезбедување на услугите на дигиталниот паричник, ниту да комбинира, односно впарува податоци за идентификација на лица или какви било други лични податоци складирани или поврзани со употребата на дигиталниот паричник со лични податоци од кои било други услуги кои ги обезбедува издавачот на дигиталниот паричник, освен ако корисникот изречно не побарал поинаку.

(3) Личните податоци кои се однесуваат на обезбедувањето на дигиталниот паричник се чуваат одвоени од сите други податоци со кои располага издавачот на дигиталниот паричник.

(4) Користењето на дигиталниот паричник е доброволно.

(5) Пристапот до услугите обезбедени од институциите на јавниот сектор или приватниот сектор, пристапот до пазарот на трудот и слободата на основање и деловно работење на ниту еден начин не смее да биде ограничена или помалку поволна за физичките или правните лица кои не користат дигитален паричник.

(6) Начинот на користење на дигиталниот паричник го пропишува министерот.

Рамка за дигитален паричник

Член 20-з

(1) Техничките правила кои се имплементираат за издавање и користење на дигиталниот паричник, односно рамка за дигитален паричник:

(а) не смее да овозможува на давателите на електронски потврди на атрибути или на која било друга страна, по издавањето на електронските потврди на атрибутите, да добиваат податоци што овозможуваат следење, поврзување или впарување на трансакциите или однесувањето на корисникот на дигитален паричник или да се добијат податоци за постоење за трансакциите или однесувањето на корисникот, освен ако корисникот не дал согласност за обработка на наведените податоци;

(б) овозможува имплементација на техники за зачувување на приватноста кои обезбедуваат неповрзаност на податоци, каде што потврда на атрибутите не бара идентификација на корисникот.

(2) Техничките правила од ставот (1) на овој член ги пропишува министерот.

Регистар на засегнати страни

Член 20-ѕ

(1) Засегната страна која има намера да овозможи употреба на дигитален паричник при обезбедување на електронски услуги го известува Министерството.

(2) Засегнатата страна од ставот (1) на овој член до Министерството треба да достави:

а) информации потребни за автентикација на дигиталните паричниции, и тоа:

- државата во која е основана засегнатата страна и

- името на засегнатата страна, нејзиниот регистарски број како што е наведено во официјалниот регистар во кој е регистрирана, вклучително и податоците за идентификација на официјалниот регистар;

б) податоци за контакт на засегнатата страна и

в) причината за употреба на дигитален паричник, вклучително и наведување на податоците што ќе ги бара од корисниците.

(3) Засегната страна не смее да бара од корисниците други податоци, освен оние со став (2) точка в) на овој член.

(4) Министерството воспоставува Регистар на засегнати страни, кој е јавен и се води во електронска форма погодна за автоматска обработка и истиот е електронски потпишан или печатиран.

(5) Засегнатата страна е должна без одлагање да го извести Министерството за секоја измена на податоците кои се содржани во Регистарот од ставот (4) на овој член.

(6) Засегнатата страна која користи дигитален паричник е должна да се идентификува пред корисникот на дигиталниот паричник.

(7) Засегнатата страна е одговорна за спроведување на постапката за автентикација и валидација на податоците за лична идентификација и електронската потврда на атрибути што ги бара од дигиталниот паричник.

(8) Засегнатата страна не смее да го одбие користењето на псевдоними, ако идентификацијата на корисникот не се бара со закон.

(9) Посредниците кои делуваат во име на засегната страна се сметаат за засегната страна и не смеат да чуваат податоци за содржината на електронската трансакција.

(10) Формата, содржината и начинот на поднесување на известувањето од ставот (1) на овој член, потребната документација од ставот (2) на овој член, како и формата, содржината и начинот на водење на Регистарот на засегнатите страни ги пропишува министерот.

(11) Техничките спецификации и процедурите за спроведување на постапката за автентикација и валидација на податоците за лична идентификација и електронската потврда на атрибути, како и употребата на псевдоними ги пропишува министерот.

Сертификација на дигитални паричници

Член 20-и

(1) Сертификација на дигиталните паричници се врши по претходна оцената на сообразност на дигиталните паричници и шемата за електронска идентификација според која тие се обезбедени согласно член 20-ж ставови (2) и (3) од овој закони и со стандардите и техничките правила од член 20-з став (2) од овој закон, од страна на телата за оцена на сообразност.

(2) Сертификацијата од ставот (1) на овој член се врши според шема за сертификација за сајбер безбедност на ниво на Европската унија, доколку шемата за сертификација за сајбер безбедност обезбедува целосна или делумна оценка на усогласеност на дигиталните паричници собарањата за сајбер безбедност утврдени согласно закон.

(3) Сертификацијата од ставот (1) на овој член важи пет години, под услов издавачот на дигиталниот паричник да врши проценка на ранливост на секои две години.

(4) Доколку при спроведување на проценката на ранливост е идентификувана ранливост и истата не е отстранета во рок од три месеци од нејзиното идентификување, издавачот на дигиталниот паричник се брише од листата на сертифицирани дигитални паричници.

(5) Усогласеноста со барањата определени во овој закон кои се поврзани со обработка на лични податоци се потврдува согласно прописите за заштитата на личните податоци.

(6) Издавачот на дигитален паричник е должен да ја достави сертификацијата од ставот (1) на овој член и проценкта на ранливост до Министерството, најдоцна во рок од 15 дена од денот на нивното добивање, односно спроведување.

(7) Листата на стандарди и процедури за сертификација на дигитален паричник ја утврдува министерот.

Листа на сертифицирани дигитални паричници

Член 20-ј

(1) Пред издавањето на дигиталните паричници, издавачите на дигитални паричници поднесуваат барање до Министерството за упис во листата на сертифицирани дигитални паричници.

(2) Во прилог кон барањето од ставот (1) на овој член, издавачите на дигитални паричници доставуваат:

- сертификат и извештај за оценка на сообразност на дигиталниот паричник,
- опис на шемата за електронска идентификација која се користи за да се обезбеди дигиталниот паричник,
- правила за надзор и информации за одговорноста на издавачот на дигиталниот паричник,
- податоци за издавачот на шемата за електронска идентификација и
- процедури за исполнетост на безбедносните услови што треба да ги исполнат издавачите на шемите за електронска идентификација кои се вклучени во процесот на издавање на дигитален паричник.

(3) Врз основа на барањето од ставот (1) на овој член и податоците и документите од ставот (2) на овој член, Министерството на својата веб-страница објавува листа на сертифицирани дигитални паричници.

(4) Во случај на промена на податоците содржани во листата од став (3) на овој член, издавачот на дигитален паричник доставува ажурирани податоци и документи до Министерството во рок од 15 дена од денот на настанувањето на промената.

(5) Министерството во рок од 30 дена од денот на доставување на податоците и документите ја ажурира листата од ставот (3) на овој член и ја објавува на веб-страницата на Министерството.

(6) Формата, содржината и начинот на поднесување на барањето од ставот (1) на овој член, како и формата, содржината на начинот на водење на листата на сертифицирани дигитални паричници ги пропишува министерот.

Нарушување на безбедноста на дигитален паричник

Член 20-к

(1) Во случаите кога е нарушена безбедноста на дигиталните паричници, техничко-технолошки средства и стандарди за валидација од член 20-д став (4) од овој закон или шемата за електронска идентификација според која се обезбедуваат дигиталните паричници или се компромитирани на начин што влијае на нивната веродостојност или на веродостојноста на други дигитални паричници, издавачот на дигиталниот паричник е должен веднаш да го суспендира обезбедувањето и користењето на дигиталните паричници, се до отстранување на причините за нарушување на безбедноста.

(2) Доколку нарушувањето на безбедноста определени од ставот (1) на овој член не се отстранат во рок од три месеци од суспензијата или во случај на сериозно нарушување на безбедноста издавачот на дигиталните паричници ќе ги повлече дигиталните паричници.

(3) Издавачот на дигитален паричник е должен да ги информира корисниците на дигиталниот паричник, засегнатите страни и Министерството, веднаш, но не подоцна од 72 часа од настанувањето на нарушувањето на безбедноста на дигиталниот паричник.

(4) Во случаите кога од нарушувањето на безбедноста се засегнати лични податоци, издавачот на дигитален паричник е должен веднаш, но не подоцна од 72 часа од настанувањето на нарушувањето на безбедноста да ја извести Агенцијата за заштита на личните податоци и соодветно да ја информира јавноста, согласно прописите за заштита на личните податоци.

(5) Министерството веднаш ги информира корисниците на дигитален паричник за секое нарушување на безбедноста што може целосно или делумно да го загрози нивниот дигитален паричник или неговата содржина.

Одговорност на издавачите на дигитален паричник

Член 20-л

(1) Издавачот на дигитален паричник е одговорен за штетата која настанала како последица од непостапување согласно овој закон, ако штетата е предизвикана намерно, од небрежност или од пропуштање на должно внимание, согласно прописите од областа на облигационите односи.

(2) Издавачот на дигиталниот паричник треба да биде осигуран од штета или да обезбеди финансиски средства согласно овој закон за одговорност за штета од употреба на шеми за електронска идентификација.

Одговорност на корисниците на дигитален паричник

Член 20-љ

Корисникот на дигиталниот паричник е должен да ги чува средствата и податоците за издавање на електронски потпис, електронски печати и дигиталниот паричник од неовластен пристап и користење и истите да ги користи согласно овој закон.

Користење на европски дигитален паричник за дигитален идентитет

Член 20-м

(1) Доколку за пристап до онлајн услуга која ја обезбедува институција од јавниот сектор е потребна електронска идентификација и автентикација, институцијата од јавниот сектор е должна да овозможи користење на европски дигитален паричник за дигитален идентитет регистриран во регистрите на сертифицирани европски дигитални паричници за дигитален идентитет, доколку корисникот на онлајн услугата ги исполнува услови за обезбедување на пристап до онлајн услугата.

(2) Кога засегната страна од приватниот сектор која обезбедува електронски услуги, освен со исклучок на микро и мали претпријатија, бара да се користи силна автентикација на корисник на електронска идентификација или доколку е потребна силна автентикација на корисникот за онлајн идентификација за договорна обврска, вклучително и во областите на транспорт, енергетика, банкарство, финансиски услуги, социјално осигурување, здравство, водоснабдување, поштенски услуги, дигитална инфраструктура, образование или телекомуникации, засегнатите страни од приватен сектор, само по барање на корисникот, овозможува користење на европски дигитални паричници за дигитален идентитет регистрани во регистрите на сертифицирани европски дигитални паричници за дигитален идентитет, доколку корисникот на електронската услуга ги исполнува услови за обезбедување на пристап до електронската услуга.

IV. ДОВЕРЛИВИ УСЛУГИ

1. Општи одредби за доверливи услуги

Вид на доверливи услуги

Член 21

(1) Доверливи услуги се услугите кои се определени како доверливи согласно со одредбите од овој закон.

(2) Квалификувани доверливи услуги се:

1) издавање на квалификувани сертификати за електронски потписи;

2) издавање на квалификувани сертификати за електронски печати;

3) издавање на квалификувани сертификати за автентичност на веб страници;

4) квалификувана доверлива услуга на зачувување на квалификувани електронски потписи;

5) квалификувана доверлива услуга на зачувување на квалификувани електронски печати;

6) квалификувана валидација на квалификуван електронски потпис;

7) квалификувана валидација на квалификуван електронски печат;

8) квалификувана доверлива услуга на издавање квалификувани електронски временски жигови;

9) квалификувана доверлива услуга на електронска препорачана достава;

10) квалификувана доверлива услуга за електронско складирање на документи и

11) квалификувана доверлива услуга за електронска потврда на атрибути;

12) квалификувана доверлива услуга за електронски записник и

13) квалификувана доверлива услуга за управување со средство за создавање на електронски потпис или печат од далечина.

(3) Давателот на доверлива услуга или давател на квалификувана доверлива услуга може да обезбеди една или повеќе услуги наведени во ставовите (1) и (2) на овој член.

Одговорност на давателите на доверлива услуга

Член 22

(1) Давател на доверлива услуга е одговорен за штетата која настанала како последица од непостапување во согласност со овој закон, ако штетата е предизвикана намерно или од небрежност.

(2) Товарот за докажување на намерата или небрежноста на давател на доверлива услуга е на физичко или правно лице кое бара надоместок на штета од ставот (1) на овој член.

(3) Кога давателите на доверлива услуга соодветно и однапред ги информираат корисниците на доверливи услуги во однос на ограничувањата за употреба на доверливите услуги кои ги обезбедуваат и кога овие ограничувања се препознатливи за трети страни, давателите на доверливи услуги не се одговорни за штетата која произлегува од користење на услугите кои ги надминуваат наведените ограничувања.

(4) Давателот на квалификувана доверлива услуга треба да биде осигуран од штета или да обезбеди финансиски средства на начин и под условите утврдени од овој закон кои важат за одговорност за штета од употреба на шеми за електронска идентификација.

Одговорност на корисниците на доверливи услуги

Член 23

Корисникот на доверливи услуги е должен да ги чува средствата и податоците за издавање на електронски потпис или печат од неовластен пристап и користење и е должен истите да ги користи во согласност со одредбите на овој закон**.**

Услови што треба да ги исполнат давателите на доверливи услуги

Член 24

(1) Давателот на неквалификувана доверлива услуга, е должен да го извести Министерството за вршење на дејност најдоцна во рок од 15 дена сметано од денот на започнувањето на вршење на дејноста.

(2) Давателот на неквалификувана доверлива услуга е должен во известувањето, покрај основните податоци за правното лице, да ги наведе и видот на услугите, техничките стандарди кои ги применува и изјава дека ќе ги почитува условите за вршење на дејноста.

(3) Министерството ги запишува во Регистарот доверливите услуги и давателот на неквалификувана услуга од ставот (2) на овој член, врз основа на поднесеното известување доколку истото ги содржи сите податоци утврдени во ставот (2) на овој член.

(4) Давател на квалификувана доверлива услуга пред да започне да ја врши својата дејност е должен да поднесе барање определено во членот 17 од овој закон за регистрација во Регистарот до Министерството.

(5) Давател на доверлива услуга за обезбедување на доверливите услуги треба да има донесено процедури и да ги преземе потребните мерки за управување со правни, деловни, оперативни или други директни или индиректни ризици поврзани со обезбедувањето на доверливите услуги и тоа:

- постапка за регистрација и начин на употреба на доверлива услуга,
- процедурални или административни проверки кои се потребни за обезбедување на доверливата услуга и
- управување и имплементација на доверливи услуги.

б) да ги извести надлежнте органи, засегнатите страни што може да се идентификуваат и јавноста, доколку тоа се бара за заштитата на јавниот интерес, за секое нарушување на безбедноста во обезбедувањето на доверливата услуга или спроведувањето на мерките наведени во точка (а) на овој став, кои може да имаат значително влијание врз обезбедувањето на доверливата услуга или заштитата на личните податоци, веднаш, а не подоцна од 24 часа откако дознале за нарушувањето на безбедноста.

(6) Техничките и организациски мерки обезбедуваат нивото на безбедност да одговара на степенот на ризик, земајќи ги предвид најновите достапни технолошки решенија, а особено се преземаат мерки за спречување и намалување на безбедносни инциденти и да се ограничат штетните ефекти од можните инциденти, како и да се информираат засегнатите страни за негативните ефекти од безбедносните инциденти.

(7) Во случај кога нарушувањето на безбедноста е поврзано со заштитата на личните податоци, давателот на доверлива услуга е должен веднаш, но не подоцна од 72 часа од настанувањето на нарушување на безбедноста да ја информира Аганцијата за заштита на личните податоци согласно прописите за заштита на личните податоци.

(8) Листата на стандарди, спецификации и процедури за обезбедување на усогласеноста со условите од став (5) на овој член ја утврдува министерот.

(9) Министерството соработува со надлежни меѓународни институции во врска со размена на информации за безбедноста и интегритетот на доверливите услуги согласно со меѓународните договори ратификувани согласно со Уставот на Република Северна Македонија.

Надлежност на Министерството за доверливи услуги и шеми за електронска идентификација

Член 25

(1)Министерството согласно со овој закон ги врши следниве задачи:

1) води Регистар на даватели на доверливи услуги и на шеми за електронска идентификација;

2) ги следи препораките од извештаите за проверка на исполнетост на условите за обезбедување на квалификувана доверлива услуга;

3) врши надзор над работата на давателите на доверливи услуги и издавачите на шеми за електронска идентификација;

4) иницира надзор пред тело за оценување на сообразноста над давателот на доверлива услуга;

5) спроведува вонредна проверка на исполнетост на условите за обезбедување на квалификувани доверливи услуги и шеми, во согласност со закон;

6) соработува со надлежниот орган за заштита на личните податоци и го известува без одлагање ако дознае дека давателите на доверливи услуги не ги почитуваат прописите за заштита на личните податоци;

7) го потврдува постоењето и правилното спроведување на плановите за престанок на вршење на дејност на давателот на доверлива услуга, вклучувајќи го и начинот на кој податоците што ги издал или добил ќе останат достапни со цел да се обезбеди континуитетот на услугата или да послужи како доказ во судска постапка;

8) соработува со органите за супервизија на Европската комисија.

9) спроведува задолжителни консултации со јавноста пред донесување на подзаконските акти определени со овој закон.

(2) Во случај на прекугранична соработка на државата, Министерството претставува единствена точка за контакт за доверливи услуги, дигитални паричници и шеми за електронска идентификација.

(3) Министерството собира податоци во врска со функционирањето на дигиталните паричници и квалификуваните доверливи услуги, и тоа за:

(а) бројот на физички и правни лица кои имаат валиден дигитален паричник;

(б) видот и бројот на услуги кои прифаќаат користење на дигитален паричник и

(в) бројот на поплаки од корисници за заштита на потрошувачите или заштита на податоци кои се однесуваат на засегнатите страни и квалификувани доверливи услуги.

(4) Министерството објавува извештај за значајни безбедносни инциденти, загрозување на податоци и засегнати корисници на дигитален паричник или на квалификувани доверливи услуги на својата веб-страница, најмалку еднаш годишно.

Надлежности на Министерството во рамки на прекугранична соработка

Член 26

Министерството во рамки на прекуграничната соработка доставува извештаи до Европската комисија за своите активности во согласност со регулативата eIDas, почнувајќи од датумот на приклучување на Република Северна Македонија како држава во рамки на надлежните органи на ниво на Европската Унија или по пристапување на Република Северна Македонија во Европската Унија.

Надлежно тело за акредитација

Член 27

(1) Министерството по претходно мислење од Институтот за акредитација на Република Северна Македонија донесува методологија за акредитација на тела за оценување на сообразност и лаборатории за тестирање на средства која ги вклучува и стандардите определени од страна на министерот.

(2) Министерството води листа на акредитирани тела за оценување на сообразност и лаборатории во Република Северна Македонија.

(3) Акредитацијата извршена од страна на надлежен орган за акредитација од земја членка на Европската Унија се признава и во Република Северна Македонија.

2. Општи одредби за квалификувани доверливи услуги

Воспоставување на односот меѓу давателот на квалификувана доверлива услуга и корисниците

Член 28

(1) Квалификувана доверлива услуга се обезбедува врз основа на склучен договор меѓу давател на квалификувана доверлива услуга и корисникот на истата, кој договор се склучува по претходно барање од страна на корисникот.

(2) Давателот на квалификувана доверлива услуга, пред склучување на договорот од ставот (1) на овој член, на јасен и недвосмилсен начин го известува лицето кое го доставило барањето за користење на квалификувана доверлива услуга за сите важни околности што се однесуваат на користењето на услугата, а особено за:

1) прописите и правилата во врска со користењето на квалификувани доверливи услуги;

2) било какви ограничувања за користење на квалификувани доверливи услуги и

3) мерките што треба да ги преземе корисникот на квалификуваните доверливи услуги и потребната технологија за безбедно користење на квалификувана доверлива услуга.

(3) Верификацијата на идентитетот на корисникот на квалификуваната доверлива услуга, пред склучување на договорот од ставот (1) на овој член, се врши со:

а) употреба на дигитален паричник или регистрирана шема за електронска идентификација на високо ниво на сигурност;

б) употреба на квалификуван сертификат за електронски потпис или печат;

в) употреба на други начини за идентификација кои обезбедуваат високо ниво на сигурност за идентификација на лица или

г) присуство на физичко лице или овластен претставник на правно лице, согласно закон.

Услови за обезбедување на квалификувани доверливи услуги

Член 29

(1) Давателот на квалификувана доверлива услуга треба да ги исполни следните услови и тоа:

1) да има вработено лица кои поседуваат потребна стручност, искуство и квалификации за примена на административни и управни постапки, кои ги исполнуваат домашните и меѓународните стандарди и кои поминале обука во областа на информатичката безбедност;

2) да биде осигуран од професионална одговорност за штета или да има обезбедено финансиски средства за надоместок на штета настаната како резултат на обезбедување на квалификувана доверлива услуга;

3) да користи безбедни системи и производи кои се заштитени од неовластени промени и гарантираат техничка сигурност и доверба во процесите што ги поддржуваат;

4) да користи безбедни системи за складирање на податоците што му се доверени, така што податоците треба да се во форма која може да се верификува и тоа:

- дека податоците ќе бидат јавно достапни единствено по претходна согласност од лицето на кого се однесуваат податоците,

- дека само овластени лица можат да прават упис или промена на зачуваните податоци,

- дека податоците можат да бидат подложни на проверка за автентичност.

5) да преземе мерки против фалсификување, кражба и неовластен пристап до податоци;

6) да ги чува и да има можност да ги направи достапни соодветен временски период, дури и по престанокот на вршење на дејноста, сите релевантни информации поврзани со податоците кои се создадени или примени од страна на давателот на квалификувана доверлива услуга, особено за обезбедување на докази во судска постапка и со цел да се обезбеди континуитетот на услугата. Складирањето на овие податоци може да се направи по електронски пат;

7) да чува навремени, точни и добро заштитени бази на податоци за издадените квалификувани електронски сертификати, доколку давателот на квалификувана доверлива услуга издава сертификати;

8) да има ажуриран план за престанок на вршење на дејност со кој ќе обезбеди континуитет во обезбедувањето на квалификувани доверливи услуги за своите корисници;

9) да преземе технички и организациски мерки за обработка на личните податоци во согласност со законите на Република Северна Македонија.

(2) Давателот на квалификувана доверлива услуга е должен да ги донесе следните акти:

1) општи услови за обезбедување на услуги кои и се достапни на јавноста;

2) процедури и постапки кои давателот на квалификувана доверлива услуга ги користи за да се обезбеди давање на услуги во согласност со прописите и општите услови наведени во точка 1) од овој став.

(3) Услов за вршење на дејноста давател на квалификувана доверлива услуга е уписот во Регистарот на доверливи услуги и шеми за електронска идентификација.

Осигурување од професионална одговорност

Член 30

Министерот го пропишува минималниот износ или видот на покритието на осигурување од ризикот од одговорност за штета причинета од страна на давателот на квалификувана доверлива услуга.

Идентификација на корисникот на квалификувани доверливи услуги

Член 31

(1) Давателот на квалификувана доверлива услуга ги верификува податоците за физичко или правно лице пред издавање на квалификуван сертификат, во согласност со закон.

(2) Проверката на податоците од ставот (1) на овој член давателот на квалификувана доверлива услуга ја врши директно или преку овластено лице во согласност со закон, на следниот начин:

1) преку лично присуство на физичкото лице или на овластениот претставник на правното лице или

2) од далечина, користејќи средства за електронска идентификација, за кои пред издавањето на квалификуваниот сертификат е обезбедено физичко присуство на физичкото лице или на овластен претставник на правното лице и кое ги исполнува условите утврдени во членот 13 од овој закон во однос на нивоата на безбедност на шемата за електронска идентификација соодветни за „значително" или „високо" или

3) преку сертификат за квалификуван електронски потпис или за квалификуван електронски печат издаден во согласност со точка 1) или 2) на овој став или

4) преку употреба на други методи за идентификација, признаени на национално ниво, кои обезбедуваат еднаква сигурност во смисла на веродостојност на физичкото присуство. Телото за оценување на сообразноста го потврдува еднаквото ниво на сигурност;

5) со начин за идентификација, употребен во земја членка на Европската Унија.

(3) Во случај на промена на податоците од ставот (1) на овој член, физичкото или правното лице е должно без одлагање, а најдоцна во рок од седум дена сметано од денот на промената, да го извести давателот на квалификувана доверлива услуга за настанатата промена.

(4) За идентификација и користење на квалификувани доверливи услуги, давателот на квалификувана доверлива услуга и издавачот на шеми за електронска идентификација може да изврши верификација користејќи го својот систем или да го интегрира својот систем на интероперабилен начин заради далечинска верификација со централниот регистар на население, документи за лична идентификација, регистри за правни лица и други лица, кога е потребно.

Оценка на условите за обезбедување на квалификувани доверливи услуги

Член 32

(1) Оценување на исполнетоста на условите за обезбедување на квалификувани доверливи услуги врши телото за оценување на сообразноста.

(2) Телото за оценување на сообразност е надлежно и за вршење на проверка на сообразност и за даватели на неквалификувана доверлива услуга, по претходна иницијатива на Министерството или по барање на давателот на услугата.

(3) По спроведување на оцената за исполнетост на услови, телото за оцена на сообразност е должно да изготви извештај за оцена на сообразност.

(4) Оценувањето за сообразност задолжително се врши пред почетокот на вршење на дејноста давател на квалификувана доверлива услуга, како и најмалку еднаш на секои 24 месеци, за секој квалификуван давател на доверливи услуги.

(5) По изготвениот извештај за спроведената оцена на сообразност на барателот или давател на квалификувана доверлива услуга, телото за оценување на сообразност извештајот го доставува до Министерството, веднаш а најдоцна во рок од три работни дена.

(6) Министерството може да побара итно преоценување на сообразноста ако постојат неправилности во обезбедувањето на квалификувани доверливи услуги или ако настанал инцидент кој значително ја загрозил или нарушил безбедноста на информациите.

(7) Цената на оценување на сообразност, вклучувајќи преоценка за итни случаи, се на товар на давателот на квалификувана доверлива услуга.

(8) Давателите на квалификувани доверливи услуги се должни да го известат Министерството најдоцна еден месец пред почетокот на планираната оцена на сообразност.

(9) Доколку давател на квалификувана доверлива услуга не успее да ги исполни условите од овој закон кои се однесуваат на даватели на квалификувани доверливи услуги, телото за оцена на сообразност определува дополнителен рок од 30 дена од овој закон.

(10) Доколку Агенцијата за заштита на личните податоци го извести Министерството дека давател на квалификувана доверлива услуга не е усогласен со прописите од областа на заштитата на личните податоци, Министерството, во согласност со степенот на неусогласеност, времетраењето и последиците од неусогласеноста, со решение го повлекува квалификуваниот статус на тој давател на квалификувана доверлива услуга за квалификуваната доверлива услуга што ја обезбедува.

(11) Министерот утврдува листа на стандарди кои треба да бидат исполнети од страна на телото за оценување на сообразност, потребна содржина на извештајот за оцена на сообразност, постапка за оценување за усогласеност со барањата, како и листа на правни лица кои се овластени во Република Северна Македонија или во земја членка на Европската Унија кои можат да вршат оценување на сообразност во Република Северна Македонија.

Постапка за упис на давател на квалификувана доверлива услуга во Регистарот

Член 33

(1) Правното лице кое има намера да обезбедува квалификувани доверливи услуги поднесува барање до Министерството за регистрација во Регистарот, пред да започне да врши дејност давател на квалификувана доверлива услуга.

(2) Во прилог на барањето од ставот (1) на овој член правното лице ги приложува и материјалите наведени како информации во барањето, вклучувајќи го и извештајот за оценување на сообразност во согласност со членот 32 од овој закон.

(3) Министерството донесува решение за регистрација на барателот во Регистарот, со кое на давателот на доверливи услуги му доделува статус на давател на квалификувана доверлива услуга, во рок од 60 дена од денот на приемот на барањето, доколку истото е целосно и во зависност од наводите од извештајот за оценување на сообразност.

(4) По исклучок на ставот (3) на овој член, кога се неопходни дополнителни проверки или прибавување на дополнителни докази за кои е потребен подолг рок, Министерството ќе го продолжи рокот за донесување на решение за регистрација во Регистарот но не подолго од 60 дена од утврдениот рок од ставот (3) на овој член.

(5) При одлучувањето, Министерството може да бара приложување и на дополнителни докази, како и да спроведе дополнителна проверка на техничките и организациски мерки и проверка на безбедносните капацитети на барателот и на услугите, во согласност со закон.

(6) Доколку барателот или услугите наведени во барањето не ги исполнуваат условите пропишани со овој закон, Министерството донесува решение за отфрлање на барањето за регистрација во регистарот по истекот на рокот утврден со став (3) или став (4) на овој член.

Престанок на вршење на дејноста давател на квалификувана доверлива услуга

Член 34

(1) Давателот на квалификувана доверлива услуга кој има намера да престане да ја врши оваа дејност е должен за намерата да ги извести корисниците на квалификувани доверливи услуги и Министерството, најдоцна три месеци пред планираниот престанок на вршење на дејноста.

(2) Давателот на квалификувана доверлива услуга кој ќе престане да ја врши оваа дејност е должен да обезбеди друг давател на квалификувана доверлива услуга кој ќе продолжи со извршувањето на овие услуги за корисниците на квалификуваните доверливи услуги и за преземените мерки веднаш, односно додека тече рокот определен во ставот (1) на овој член ќе го извести Министерството.

(3) Давателот на квалификувана доверлива услуга е должен да ја достави целокупната документација и сите потребни технички средства во согласност со закон, во однос на обезбедување на услуги од страна на друг давател на квалификувана доверлива услуга на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги.

(4) Доколку давателот на квалификувана доверлива услуга не постапи во согласност со обврската утврдена во ставовите (2) и (3) на овој член, Министерството ќе побара од давателот на квалификувана доверлива услуга без одлагање до министерството да ја достави целокупната документација и опрема, вклучително и процедурите за постапување со истите.

(5) Министерството привремено ќе ја чува документацијата и опремата, сè до обезбедување на друг давател на квалификувана доверлива услуга кој ќе продолжи да ги извршува овие услуги за корисниците, за сметка на давателот на квалификувана доверлива услуга кој престанува да ја врши оваа дејност.

(6) Начинот и Процедурата за чувањето на документацијата и опремата, ги пропишува министерот.

(7) Во случај на привремена забрана за вршење на дејност квалификуван давател на доверливи услуги, квалификуваните сертификати издадени пред денот на стапувањето во сила на забраната, остануваат во важност.

Листа на даватели на квалификувани доверливи услуги

Член 35

(1) Министерството ја објавува листа на даватели на квалификувани доверливи услуги, како и листа на квалификувани доверливи услуги кои тие ги обезбедуваат на својата веб страница, во електронска форма која е погодна за автоматска обработка.

(2) Листата од ставот (1) на овој член е потпишана со електронски потпис или запечатена со електронски печат на Министерството.

(3) Податоците во листата на даватели на квалификувани доверливи услуги произлегуваат од Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација, како и податоци преземени со користење на автоматски средства.

(4) Формата и начинот на објавување на листата од ставот (1) на овој член ја пропишува министерот.

Ознака за доверба на квалификувана доверлива услуга

Член 36

(1) Ознаката за доверба на квалификувана доверлива услуга (во натамошниот текст: како ознака за доверба) е знак кој е едноставен, препознатлив и јасно укажува на квалификувана доверлива услуга, чија форма, содржина и лого се утврдени со ставот (3) на овој член.

(2) Давателите на квалификувани доверливи услуги имаат право да ја користат ознаката за доверба за квалификувана доверлива услуга за која се регистрирани и истата се должни да ја поврзат со листата на квалификувани даватели на доверливи услуги.

(3) Министерот ги пропишува формата, структурата, големината и логото на ознаката за доверба на квалификувана доверлива услуга.

Ознака за доверба на дигитален паричник

Член 36-а

(1) Ознаката за доверба на дигитален паричник е знак кој е единствен, препознатлив и јасно укажува на дигиталниот паричник.

(2) Издавачот на дигиталниот паричник има право да ја користи ознаката за доверба и е должен да ја поврзе со листата за сертификација на дигитални паричници.

(3) Формата, структурата, големината и логото на ознаката за доверба за дигитален паричник ја пропишува министерот.

Прекугранично признавање на даватели на доверливи услуги

Член 37

(1) На давател на доверлива услуга регистриран со седиште во странска држава му се признава статусот давател на доверливи услуги во Република Северна Македонија доколку истиот е регистриран во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација.

(2) Давателите на доверлива услуга кои се основани од земја членка на Европската Унија и се запишани во Листата на доверливи услуги на Европската Унија, можат да работат и да обезбедуваат услуги на територијата на Република Северна Македонија, без претходна регистрација во Регистарот на даватели на доверливи услуги и шеми за електронска идентификација.

(3) Давателите на квалификувани доверливи услуги регистрирани со седиште во Република Северна Македонија, а кои се регистрирани во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација, се правно еквивалентни на квалификуваните доверливи услуги обезбедени од страна на давателите на квалификувани доверливи услуги основани во Европската Унија, врз основа на претходно склучен договор меѓу Република Северна Македонија и Европската Унија.

(4) Со договорот наведен во ставот (3) на овој член особено се гарантира дека:

(а) барањата применливи за даватели на квалификувани доверливи услуги основани во Европската Унија и за квалификуваните доверливи услуги кои тие ги обезбедуваат, се исполнети од страна на давателите на доверливи услуги во Република Северна Македонија и

(б) квалификуваните доверливи услуги обезбедени од страна на квалификуваните даватели на доверливи услуги основани во Европската Унија, се признати како правно еквивалентни на доверливите услуги обезбедени од страна на давателите на доверливи услуги во Република Северна Македонија.

V. ЕЛЕКТРОНСКИ ПОТПИС И ЕЛЕКТРОНСКИ ПЕЧАТ

1. Напреден електронски потпис

Услови кои треба да ги исполни напредниот електронски потпис

Член 38

Напредниот електронски потпис треба:

1) да биде на единствен начин поврзан со потписникот;

2) да овозможи идентификација на потписникот;

3) да е создаден со податоци за создавање на електронски потпис кои потписникот, со високо ниво на доверба, може да ги користи единствено под сопствена контрола;

4) да е поврзан со податоци кои се потпишани на таков начин што секоја подоцнежна измена на истите е воочлива.

2. Напреден електронски печат

Услови кои треба да ги исполни напредниот електронски печат

Член 39

Напредниот електронски печат треба:

1) да биде на единствен начин поврзан со создавачот на печатот;

2) да овозможи идентификација на создавачот на печатот;

3) да е создаден со податоци за создавање на електронски печат кои создавачот на печатот, со високо ниво на доверба, може да ги користи единствено под сопствена контрола;

4) да е поврзан со податоците кои ги запечатува на таков начин што секоја подоцнежна измена на истите е воочлива.

3. Содржина на квалификуван сертификат за електронски потпис и печат

Член 40

(1) Стандардите кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат ги пропишува министерот.

(2) Покрај стандардите од ставот (1) на овој член кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат, можат да содржат и дополнителни податоци кои нема да влијаат врз интероперабилноста и признавањето на квалификуваниот електронски потпис и квалификуваниот електронски печат.

Правна и доказна сила на квалификуваните сертификати за електронски потпис и печат

Член 41

Квалификуваните сертификати за електронски потпис и печат издадени од квалификуваните даватели на доверливи услуги имаат иста правна и доказна сила како јавните исправи.

Укинување или суспензија на квалификуван сертификат за електронски потпис, за електронски печат и за автентичност на веб страница

Член 42

(1) Давателот на квалификувана доверлива услуга кој го издава квалификуваниот сертификат за електронски потпис, за електронски печат и за автентичност на веб страница е должен да го укине издадениот квалификуван сертификат, доколку:

1) сопственикот на сертификатот за квалификуван електронски потпис, за електронски печат или за автентичност на веб страница поднесе барање за поништување на сертификатот;

2) сопственикот на сертификатот ја загуби деловната способност или престанал да постои или се променети околности кои влијаат на валидноста на сертификатот;

3) утврди дека недостасуваат податоци во сертификатот;

4) утврди дека податоците за создавање на квалификуван електронски потпис, за квалификуван електронски печат или за автентичност на веб страница или системот на давателот на квалификувана доверлива услуга е компромитиран на начин кој влијае врз безбедноста и сигурноста на сертификатите;

5) утврди дека податоците за создавање на електронски потпис, за електронски печат или за автентичност на веб страница или системот преку кој се извршува електронска трансакција се изложени на ризик, на начин кој влијае на сигурноста и безбедноста на електронскиот потпис, електронскиот печат или веб страницата и

6) настане престанок на правно лице, под услови утврдени со закон.

(2) Давателот на доверлива услуга кој го издава квалификуваниот сертификат за електронски потпис, за електронски печат или за автентичност на веб страница го известува корисникот на квалификуваната доверлива услуга за поништување на сертификатот во рок од 24 часа од приемот на барањето или од настанувањето на околностите кои се основ за поништување на сертификатот.

(3) Ако квалификуваниот сертификат за електронски потпис, за електронски печат или за автентичност на веб страница биде укинат после првичното издавање, тогаш ја губи важноста од моментот на укинување и неговиот статус на квалификуван сертификат не може да биде вратен под никакви околности.

(4) Давателите на квалификувани доверливи услуги кои издаваат квалификувани сертификати, на секоја засегната страна и обезбедуваат информации за валидноста, суспензијата или укинувањето на издадените квалификувани сертификати.

(5) Информациите од ставот (4) на овој член се ставаат на располагање на секоја засегната страна најмалку за поединечните сертификати, во секое време и по истекот на периодот на нивната важност, на автоматски начин кој е сигурен, ефикасен и без надоместок.

(6) Корисникот на квалификувана доверлива услуга е должен да побара укинување на издадениот сертификат за квалификуван електронски потпис, за квалификуван електронски печат и за автентичност на веб страница од неговиот издавач во случај на губење, оштетување или загрозување на интегритетот на податоците од сертификатот или доколку настане промена на податоците за креирање сертификати.

(7) Во случај на суспензија на сертификат за квалификуван електронски потпис, за електронски печат и за автентичност на веб страница истиот губи важност за времетраење на периодот на важноста на суспензијата.

(8) Информациите за суспензија и нејзиното времетраење за квалификуван сертификат за електронски потпис, за електронски печат или за автентичност на веб страница или за укинување на истите ќе бидат внесени во базата на податоци на издадени квалификувани сертификати кои се чуваат од страна на давателот на квалификувана доверлива услуга и истите ќе бидат видливи при проверка на статусот на валидност на квалификуван електронски сертификат.

Евиденција на издадени и укинати сертификати за квалификуван електронски потпис, за електронски печат и за автентичност на веб страница

Член 43

(1) Издавачот на квалификувани сертификати за електронски потпис, за електронски печат или за автентичност на веб страница е должен да ја чува целокупната документација за издадените и укинатите квалификувани сертификати за електронски потпис, за електронски печат или за автентичност на веб страница, како и средствата за електронска идентификација и верификација во административни, правни и други процедури, најмалку десет години по истекот на рокот за кој е издаден на сертификатот или по неговото укинување.

(2) Обврската од ставот (1) на овој член се однесува и на суспензија на квалификуваните сертификати за електронски потпис, за електронски печат или за автентичност на веб страница.

(3) Податоците од ставот (1) на овој член може да се чуваат и во електронска форма.

Средства за создавање на квалификуван електронски потпис или квалификуван електронски печат

Член 44

(1) Создавањето или управувањето со податоци за создавање електронски потпис или дуплирање на податоците за создавање електронски потпис заради воспоставување на резервна копија ја врши давател на квалификувана доверлива услуга за управување со квалификувано средство за создавање електронски потпис или печат од далечина, во име на потписникот, на негово барање.

(2) Техничките стандарди кои треба да бидат исполнети од страна на давателите на квалификувана доверлива услуга, како и начинот на создавање на квалификувани електронски потписи или квалификувани електронски печати ги пропишува министерот.

Услови за обезбедување на квалификувана доверлива услуга за управување со квалификувани средства за создавање електронски потпис или печат од далечина

Член 44-а

(1) Управувањето со средства за создавање на квалификуван електронски потпис или печат од далечина го врши само давател на квалификувана доверлива услуга за управување со средства за создавање на квалификуван електронски потпис или печат од далечина, кој:

(а) создава или управува со податоци за создавање електронски потпис во име на потписникот;

(б) ги дуплира податоците за создавање електронски потпис заради воспоставување на резервни копии, под услов да се исполнети следниве барања:

- безбедноста на дупликатите на збирки на податоци задолжително да биде на исто ниво на безбедност како и за оригиналните збирки на податоци и
- бројот на дуплирани збирки на податоци не смее да го надмине минимумот потребен за да се обезбеди континуитет на услугата и

(в) ги исполнува сите барања определени во потврдата за сообразност на средството за создавање на квалификуван електронски потпис од далечина, издадена согласно член 45 од овој закон.

(2) Техничките стандарди, спецификации и процедури за управување со средства за создавање на квалификуван електронски потпис или печат од далечина ги пропишува министерот.

Сообразност на средствата за создавање на квалификуван електронски потпис или квалификуван електронски печат

Член 45

(1) Оцена на исполнетост на техничките стандарди што се однесуваат на средствата за издавање на квалификувани електронски потписи или квалификувани електронски печати врши акредитирана лабораторија.

(2) Лабораторијата издава потврда за сообразност на средство за создавање на квалификувани електронски потписи или квалификувани електронски печати и за истото го известува Министерството најдоцна во рок од седум дена, сметано од денот на издадената потврда за средствата.

(3) Техничките стандарди кои треба да бидат исполнети, а кои се предмет на оцена на исполнетост на технички барања од страна на овластеното тело се пропишани со актот донесен врз основа на членот 44 од овој закон.

(4) Министерството води листа на средства за создавање на квалификуван електронски потпис или квалификуван електронски печат, врз основа на податоците добиени од потврдите од лабораторијата.

(5) Лабораторијата без одлагање, а најдоцна во рок од седум дена од денот на настаната промена е должна да го извести Министерството за издавање или одземање на потврда за сообразност на средствата за создавање на квалификувани електронски потписи и квалификувани електронски печати.

(6) Министерот ја пропишува содржината и начинот на водењето на листата од ставот (4) на овој член, начинот на поднесување на барање за регистрација во листата, потребните документи со барањето, како и начинот за регистрација во листата.

(7) Содржината на потврдата за сообразност на средство за создавање на квалификувани електронски потписи или квалификувани електронски печати и начинот на нејзино издавање ја пропишува министерот.

(8) Средствата од ставот (1) на овој член кои се сертифицирани во акредитирани лаборатории во земја членка на Европската Унија се признаваат и во Република Северна Македонија.

(9) Валидноста на потврдата за сообразност на средство за создавање на квалификувани електронски потписи или квалификувани електронски печати е пет години, под услов издавачот на средството да врши проценка на ранливост на секои две години.

(10) Доколку при спроведување на проценката на ранливост е идентификувана ранливост и истата не е отстранета во рок од три месеци од нејзиното идентификување, валидноста на потврдата од ставот (9) на овој член престанува да важи.

4. Квалификувана доверлива услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат

Валидација на квалификуван електронски потпис или квалификуван електронски печат

Член 46

(1) Процесот на валидација на квалификуван електронски потпис или квалификуван електронски печат се спроведува со цел да се утврди:

1) дали сертификатот кој се однесува на квалификуван електронски потпис или печат во времето на потпишувањето или создавањето на печатот претставува квалификуван електронски сертификат;

2) дали квалификуваниот сертификат бил издаден од давател на квалификувана доверлива услуга и бил валиден во времето на потпишување или запечатување;

3) дали податоците за валидација на потписот или печатот се соодветни со податоците дадени на засегнатата страна;

4) дали единствениот збир на податоци во квалификуваниот сертификат кои го претставуваат потписникот или создавачот на печатот, кои се дадени на засегната страна, се точни;

5) дали во случај на користење на псевдоним во времето на потпишување или запечатување истото и е јасно укажано на засегнатата страна;

6) дали електронскиот потпис или електронскиот печат бил создаден од средство за создавање на квалификуван електронски потпис или квалификуван електронски печат;

7) дали интегритетот на податоците кои се потпишани или запечатени не е компромитиран;

8) дали ги исполнуваат условите пропишани со членовите 38 и 39 од овој закон во времето на потпишување или запечатување.

(2) Системот кој се користи за валидација на квалификуван електронски потпис или на електронски печат на засегнатата страна и го обезбедува точниот резултат на процесот на валидација и ѝ овозможува идентификување на сите проблеми од значење за сигурноста.

Услови за обезбедување на квалификувана услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат

Член 47

(1) Квалификувана услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат може да биде обезбедена единствено од давател на квалификувана доверлива услуга и тоа:

1) процесот за валидација на квалификуван електронски потпис или квалификуван електронски печат е спроведен во согласност со членот 46 од овој закон;

2) на засегнатата страна и овозможува да добие потврда од процесот на валидација на автоматизиран начин, кој е сигурен и ефикасен;

3) дека потврдата од процесот на валидација од точката 2) од овој став е запечатена со напреден електронски печат или потпишана со напреден електронски потпис од давателот на квалификуваната доверлива услуга.

(2) Потврдата за валидација на квалификуван електронски потпис или квалификуван електронски печат издадена од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

(3) Стандардите кои треба да ги содржат потврдите за валидација на квалификуван електронски потпис или квалификуван електронски печат ги пропишува министерот.

Услови за валидација на напредни електронски потписи или електронски печати засновани на квалификувани сертификати

Член 47-а

(1) Процесот за валидација на напреден електронски потпис или електронски печат заснован на квалификуван сертификат ја потврдува валидноста на напредниот електронски потпис или напредниот електронски печат заснован на квалификуван сертификат, под услов:

(а) сертификатот што го поддржува потписот или печатот во моментот на потпишувањето или печатирањето да бил квалификуван сертификат за електронски потпис или печат кој е во согласност со одредбите од овој закон кои се однесуваат на квалификувани сертификати за електронски потписи или печати;

(б) квалификуваниот сертификат бил издаден од давател на квалификувана доверлива услуга за издавање на квалификувани електронски потписи или печати и бил важечки во моментот на потпишувањето, односно печатирањето;

(в) податоците за валидација на потписот или печатот одговараат на податоците доставени до засегнатата страна;

(г) сетот на податоци што го претставуваат потписникот, односно употребувачот на печатот во сертификатот е правилно доставен до засегната страна;

(д) употребата на кој било псевдоним е јасно означена на засегната страна доколку псевдоним бил користен во моментот на потпишувањето;

(ѓ) интегритетот на потпишаните или печатираните податоци не е загрозен и

(е) условите определени со член 38 или член 39 од овој закон биле исполнети во моментот на потпишувањето, односно печатирањето.

(2) Системот составен од техничко-технолошки средства што се користи за валидација на напредниот електронски потпис или напреден електронски печат заснован на квалификуван сертификат, на засегнатата страна и обезбедува точен резултат од процесот на валидација и оневозможува нарушување на безбедноста.

(3) Техничките стандарди, спецификации и процедури за валидација на напредните електронски потписи засновани на квалификувани сертификати ги пропишува министерот.

5. Квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати

Услови за обезбедување на квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати

Член 48

(1) Квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати може да биде обезбедена единствено од давател на квалификувана доверлива услуга кој користи процедури и технологии оспособени да ја продолжат веродостојноста на квалификуваниот електронски потпис или квалификуваниот електронски печат и по истекот на период на важење обезбеден преку користење на технолошки средства.

(2) Стандардите кои треба да ги исполни квалификуваната доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати ги пропишува министерот со правилник.

Правно дејство на електронскиот потпис

Член 49

(1) Не може да се оспорува доказната сила на електронскиот потпис само затоа што е употребен во електронски облик или затоа што ги исполнува условите за квалификуван електронски потпис.

(2) Квалификуваниот електронски потпис има иста правна и доказна сила како и своерачниот потпис.

Правно дејство на електронскиот печат

Член 50

(1) Не може да се оспорува доказната сила на електронскиот печат само затоа што е употребен во електронски облик или затоа што ги исполнува условите за квалификуван електронски печат.

(2) Квалификуваниот електронски печат е основа за презумција за интегритетот на податоците и за точноста на потеклото на податоците со кои истиот е поврзан.

6. Електронски временски жиг

Услови кои треба да ги исполни квалификуваниот електронски временски жиг

Член 51

(1) Квалификуваниот електронски временски жиг ги исполнува следните услови:

1) го поврзува датумот и времето со податоците на таков начин што разумно може да се претпостави дека можноста податоците да бидат незабележано променети е исклучена;

2) се заснова на прецизен извор за време поврзан со утврден меѓународен стандард за време;

3) запечатен е со напреден електронски печат или потпишан со напреден електронски потпис од давателот на квалификувана доверлива услуга.

(2) Стандардите кои треба да ги исполнат квалификуваните електронски временски жигови ги пропишува министерот.

Правно дејство на електронските временски жигови

Член 52

(1) Не може да се оспорува доказната сила на електронскиот временски жиг само затоа што е употребен во електронски облик или затоа што ги исполнува условите за квалификуван електронски временски жиг.

(2) Квалификуваниот електронски временски жиг е основа за презумција за точноста на датумот и времето кои се означени, како и интегритетот на податоците на кои се однесуваат датумот и времето.

(3) Квалификуваниот сертификат за електронски временски жиг издаден од дател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

7. Електронска достава

Услови за вршење на квалификувана електронска препорачана достава

Член 53

(1) Квалификуваната електронска препорачана достава ги исполнува следните услови:

1) да е обезбедена преку еден или повеќе даватели на квалификувана доверлива услуга;

2) да обезбеди високо ниво на сигурност за идентификација на испраќачот;

3) да обезбеди идентификација на примачот пред доставата на податоците;

4) да обезбеди сигурност во процесот на праќање и примање на податоци преку употреба на напреден електронски потпис или напреден електронски печат на давателот на квалификувана доверлива услуга на таков начин што ќе се спречи можноста при евентуална промена на податоците да останат незабележани;

5) обезбеди сигурна размена на податоци која е соодветна на целите на испраќање и примање на податоци, а преку која ќе може јасно да се определи испраќачот и примачот на податоците;

6) да обезбеди сигурност дека времето и датумот на испраќање, примање и можните промени на податоците е јасно означено преку употреба на електронски временски жиг;

7) да обезбеди сигурност дека се исполнети условите поединечно за секој давател на услуга за електронска препорачана достава во случаите кога податоците се пренесуваат меѓу два или повеќе даватели на услуга за електронска препорачана достава.

(2) Давателите на квалификувана доверлива услуги за квалификувана електронска препорачана достава може да се договорат за интероперабилноста помеѓу квалификуваните доверливи услуги за квалификувана електронска

препорачана достава што тие ги обезбедуваат, под услов договорената рамка за интероперабилност да е сообразна на барањата определени во ставот (1) на овој член и истата да е потврдена од тело за оцена на сообразност.

(3) Стандардите кои ги содржат потврдите за квалификувана електронска препорачана достава ги пропишува министерот.

Правно дејство на електронска препорачана достава

Член 54

(1) Не може да се оспорува доказната сила на податоците испратени или примени преку електронска препорачана достава само затоа што се во електронски облик или затоа што ги исполнуваат условите за квалификувана електронска препорачана достава.

(2) Користењето на квалификувана електронска препорачана достава за примање или праќање на податоци е основа за презумпција на интегритетот на тие податоци, испраќањето на истите од утврдениот испраќач, нивниот прием од утврдениот примач, како и точноста на датумот и времето на испраќање и примање на тие податоци означени од давателот на услугата квалификувана електронска препорачана достава.

(3) Потврдата за квалификувана електронска препорачана достава издадена од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

8. Проверка на автентичност на веб страници

Квалификуван сертификат за автентичност на веб страници

Член 55

Стандардите кои треба да ги исполнува квалификуваниот сертификат за автентичност на веб страници ги пропишува министерот.

Правна и доказна сила на квалификуваниот сертификат за автентичност на веб страници

Член 56

Квалификуваниот сертификат за автентичност на веб страници издаден од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа.

Квалификуваниот сертификат за автентичност на веб-страници издаден од давател на квалификувана доверлива услуга регистриран во Европската Унија или во земја членка на унијата се признава како да е издаден од домашно правно лице.

Превентивни мерки за сајбер безбедност

Член 56-а

(1) Издавачите на веб-прелистувачи не смеат да наметнуваат дополнителни барања за сертификатите за автентичност на веб-страници, освен барањата определени со стандардите кои треба да ги исполнува квалификуваниот сертификат за автентичност на веб-страница.

(2) Издавачите на веб-прелистувачи нема да преземат никакви мерки спротивни на барањата од ставот (1) на овој член, особено во однос на барањата за признавање на квалификувани сертификати за автентикација на веб-страници од член 55 од овој закон, како и за барањата за прикажување на податоците за идентитетот кои треба да се обезбедени на начин лесен за користење.

(3) По исклучок на ставот (1) од овој член, во случај на нарушувања на безбедноста или губење на интегритетот на идентификуван сертификат или збир на сертификати, издавачите на веб-прелистувачи можат да преземат мерки на претпазливост во однос на тој сертификат или збир на сертификати.

(4) Кога издавачот на веб прелистувач презема мерки на претпазливост во согласност со ставот (3) на овој член, истиот е должен веднаш писмено да го извести Министерството и субјектот на кој му е издаден сертификатот за автентичност на веб-страници, за преземените мерки за намалување на ризиците поврзани со сајбер безбедноста.

(5) Министерството презема мерки врз основа на наводите содржани во известувањето од ставот (4) на овој член, доколку по утврдено нарушување на безбедноста не биде повлечен квалификуваниот сертификат за автентичност на веб-страници.

(6) Министерството го известува издавачот на веб-прелистувачот за укинување на мерките преземени согласно ставот (3) на овој член.

9. Електронско складирање на документи

Подготовка на документи за електронско складирање

Член 57

(1) Подготвката на документи за електронско складирање се однесува на:

1) документи кои првично биле создадени во електронска форма погодна за електронско складирање;

2) конверзија на електронски документ во поинаков формат погоден за електронско складирање;

3) дигитализација на документи изворно создадени во форма која не е електронска, погодни за електронско складирање.

(2) Во документот подготвен за електронско складирање, може да бидат вклучени и метаподатоци, по избор на лицето кое врши подготовка на документи за електронско складирање или заради потребите на самиот процес.

Подготовка на документи за сигурносно електронско складирање и квалификувано сигурносно електронско складирање

Член 58

(1) При подготовката на документи за сигурносно електронско складирање треба да бидат исполнети следните услови:

1) обезбеди сигурност дека сите основни елементи на содржината на оригиналниот документ се верно пренесени во документот подготвен за електронско складирање, земајќи ги предвид природата и целта на документот, односно да се зачува интегритет на содржината на документот;

2) обезбеди сигурност дека ќе се зачува употребливоста на оригиналниот документ;

3) обезбеди сигурност дека се вклучени сите елементи на содржината на оригиналниот документ што се од значење за неговата автентичност;

4) обезбеди сигурност за интегритетот на оригиналниот документ, како и за неговите прилози, на начин што се употребени електронски потпис или печат и електронски временски жиг;

5) спроведе контрола на точност и квалитет при процесот на конверзија, со цел да се отстранат секакви грешки кои би можеле да бидат предизвикани од овој процес;

6) се осигура дека за активностите преземени во подготовката на документите за сигурносно електронско складирање се води уредна евиденција.

(2) Доколку пропишаниот рок за чување на документите согласно со закон е подолг од пет години, тогаш документот подготвен за сигурносно електронско складирање треба да биде во формат кој е погоден за долгорочно чување.

(3) Подготовката на документи за квалификувано сигурносно електронско складирање задолжително треба да:

1) обезбеди сигурност дека сите основни елементи на содржината на оригиналниот документ се верно пренесени во документот подготвен за електронско складирање, земајќи ги предвид природата и целта на документот, односно да се зачува интегритет на содржината на документот;

2) обезбеди сигурност дека ќе се зачува употребливоста на оригиналниот документ;

3) обезбеди сигурност дека се вклучени сите елементи на содржината на оригиналниот документ што се од значење за неговата автентичност;

4) обезбеди сигурност дека за интегритетот на оригиналниот документ, како и за неговите прилози, се употребени квалификуван електронски потпис или квалификуван електронски печат и квалификуван електронски временски жиг;

5) спроведе контрола на точност и квалитет при процесот на конверзија, со цел да се отстранат секакви грешки кои би можеле да бидат предизвикани од овој процес;

6) се осигура дека за активностите преземени во подготовката на документите за сигурносно електронско складирање се води уредна евиденција.

(4) Доколку пропишаниот рок за чување на документите согласно со закон е од трајна вредност, тогаш документот подготвен за квалификувано сигурносно електронско складирање треба да биде во формат кој е погоден за долгорочно чување.

(5) Владата, на предлог на Министерството ги пропишува поблиските услови за подготовка на документите за електронско складирање и квалификувано електронско складирање и форматите на документите кои се погодни за складирање.

Сигурносно електронско складирање и квалификувано сигурносно електронско складирање на документи

Член 59

(1) Сигурносно електронско складирање на документи кои во нивната оригинална форма содржат електронски потпис или печат, а со цел да се потврди интегритетот и потеклото на овие документи, треба да се подготват на тој начин што за време на нивното складирање се користат востановени процедури и технолошки решенија.

(2) Сигурносно електронско чување на документи кои се изготвени согласно со членот 58 од овој закон, на кои е нанесен електронски потпис или печат и електронски временски жиг на начин определен во членот 58 став 1 точка 4) од

овој закон со цел да се потврди интегритетот на оригиналниот документ, како и на неговите прилози, се врши така што во текот на постапката за складирање се користат востановени технолошки решенија.

(3) Квалификувано сигурносно електронско складирање на документи кои во нивната оригинална форма содржат квалификуван електронски потпис или квалификуван електронски печат, а со цел да се потврди интегритетот и потеклото на овие документи, треба да се подготват на тој начин што за време на нивното складирање се користат востановени процедури и технолошки решенија.

(4) Сигурносно електронско чување на документи кои се изготвени согласно со членот 58 од овој закон, на кои е нанесен квалификуван електронски потпис или квалификуван електронски печат и квалификуван електронски временски жиг на начин определен во членот 58 став 2 точка 4) од овој закон со цел да се потврди интегритетот на оригиналниот документ, како и на неговите прилози.

(5) Министерот пропишува методологија за имплементација на процедурите и технолошки решенија.

Услуги за електронско складирање и квалификувано електронско складирање на документи

Член 60

(1) Услуги за електронско складирање на документи ги обезбедува давател на доверливи услуги, кој има преземено соодветни технички и организациски мерки преку кои обезбедува сигурност на електронско складирање на документи, согласно со одредбите од овој закон.

(2) Давателот на услуги за електронско складирање на документи може да се ограничи на складирање на документи кои во нивната оригинална форма содржат електронски потпис или печат.

(3) За документ кој се чува во рамките на услугите на електронско складирање на документи постои презумпција за верност на оригиналниот документ, за кој давателот на услугата електронско складирање на документи издава соодветен сертификат, согласно со одредбите од овој закон.

(4) Ако документот е зачуван со користење на услугите за електронско складирање на документи, така што периодот на складирање е подолг од пропишаниот период на чување на оригиналниот документ согласно со прописите од областа на архивското работење, тогаш оригиналниот документ може да биде уништен, освен ако не е поинаку определено со закон.

(5) Услуги за квалификувано електронско складирање на документи ги обезбедува давател на квалификувана доверлива услуга, кој има преземено соодветни технички и организациски мерки преку кои обезбедува сигурност на квалификуваното електронско складирање на документи, во согласност со одредбите од овој закон.

(6) Давателот на услуги за квалификувано електронско складирање на документи може да се ограничи на складирање на документи во кои нивната оригинална форма содржат квалификуван електронски потпис или квалификуван електронски печат.

(7) За документ кој се чува во рамките на услугите на квалификувано електронско складирање на документи, во правиот промет се смета за верен на оригиналниот документ, за кој давателот на услугата квалификувано електронско складирање на документи издава соодветен сертификат согласно со одредбите од овој закон.

(8) Ако документот е зачуван со користење на услугите за квалификувано електронско складирање на документи, така што периодот на складирање е подолг од пропишаниот период на чување на оригиналниот документ, тогаш оригиналниот документ може да биде уништен, освен ако не е поинаку определено со закон.

(9) Министерот ги пропишува стандардите за електронско складирање и квалификувано електронско складирање на документи.

10. Електронската потврда на атрибути

Правно дејство на електронската потврда на атрибути

Член 60-а

(1) Електронска потврда на атрибути и потврдата на атрибути која е издадена од институција од јавен сектор или од давател на квалификувана доверлива услуга во име на институција од јавен сектор има иста правна и доказна сила како јавна исправа.

(2) Не може да се оспорува доказната сила на електронската потврда на атрибути затоа што е издадена во електронска форма или затоа што не ги исполнува условите за квалификувани електронски потврди за атрибути.

(3) Податоците за идентификација на лицето содржани во електронската потврда на атрибути не може да ја заменат електронската идентификација со средство за електронска идентификација за пристап до електронска услуга која е обезбедена од институција од јавниот сектор, освен ако со закон поинаку не е определено.".

Услови што треба да ги исполни квалификуваната електронска потврда на атрибути

Член 60-б

(1) Доколку квалификуваната електронска потврда на атрибути е повлечена по нејзиното издавање, престанува да важи од моментот на повлекувањето и нејзиниот статус не може да биде вратен.

(2) Квалификуваната електронска потврда на атрибути не смее да биде предмет на дополнителни услови, освен условите што се однесуваат за обезбедување на квалификувана доверлива услуга и стандардите од подзаконскиот акт од ставот (1) на овој член.

(3) Стандардите кои треба да ги исполни квалификиуваната електронска потврда на атрибути како и минималната листа на податоци содржана во квалификуваната електронска потврда на атрибути ги пропишува министерот.

(4) Стандардите и процедурите за квалификувано електронско потврдување на атрибути кои се поврзани со издавањето на дигиталниот паричник ги пропишува министерот.

Верификација на атрибути од изворник на податоци

Член 60-в

(1) Институцијата од јавниот сектор чиј репозиториум или систем е автентичен извор на атрибути претставува изворник на податоци кои се содржани во електронската потврда на атрибути.

(2) Институциите од јавниот сектор кои се јавуваат во својство на изворници на податоци преземаат мерки со кои им се овозможува на давателите на квалификувани доверливи услуги за издавање на електронски потврди на атрибути да ги верификуваат атрибутите со употреба на електронски средства, на барање на корисниците согласно овој закон.

(3) Министерството воспоставува и води каталог на атрибути и автентични извори.

(4) Каталогот од ставот (3) на овој член се води во електронска форма и е јавно достапен.

(5) Стандардите, спецификациите и процедурите за каталогот на атрибути, како и шемите за потврдување на атрибутите и процедурите за верификација на квалификуваните електронски потврди на атрибути ги пропишува министерот.

Услови за електронска потврда на атрибути издадена од или во име на изворник на податоци

Член 60-г

(1) Електронската потврда на атрибути издадена од или во име на изворник на податоци треба да:

(а) ги исполнува стандардите пропишани со подзаконскиот акт од член 60-б став (1) од овој закон и

(б) има квалификуван сертификат за електронски потпис или квалификуван сертификат за електронски печат на изворникот на податоци, определен како автентичен извор во Каталогот на атрибути и автентични извори, кој содржи сет на сертифицирани атрибути во форма погодна за автоматска обработка и:

- податоци со кои јасно се укажува дека изворникот на податоци е основан согласно закон и е одговорен за автентичниот извор на атрибутот, врз основа на кој се издава електронската потврда на атрибутите или е давател на квалификувана доверлива услуга за издавање на електронска потврда на атрибути кој дејствува во име на изворникот,

- обезбедува збир на податоци кои недвосмислено го претставуваат автентичниот извор наведен претходната алинеја и

- податок за идентификација на законот со кој е основан изворникот на податоци.

(2) Институциите од јавниот сектор кои се автентичен извор на атрибути и кои издаваат електронски потврди на атрибути го исполнуваат нивото на сигурност и доверба еднакво на давателите на квалификувани доверливи услуги определено со овој закон.

(3) Институциите од јавниот сектор кои се автентичен извор на атрибути до Министерството доставуваат известување за упис Каталогот на автентични извори и атрибути, со прилог извештај за оцена на сообразност, издаден од тело за оцена на сообразност.

(4) Институциите од јавниот сектор кои се изворници на податоци до Министерството доставуваат известување за упис во Каталогот на автентични извори и атрибути.

(5) Електронската потврда за атрибути издадена од или во име на институција од јавниот сектор се смета дека е во согласност со условите од ставот (1) на овој член, доколку истата е издадена во согласност со стандардите, спецификациите и процедурите од ставот (6) на овој член.

(6) Стандардите, спецификации и процедури за електронско потврдување на атрибути издадени од или во име на институција од јавниот сектор ги пропишува министерот.

(7) Институциите од јавниот сектор кои издаваат електронски потврди на атрибути обезбедуваат интерфејс за издавачите на дигиталните паричници.

Издавање на електронски потврди на атрибути во дигитални паричници

Член 60-д

(1) Издавачите на електронски потврди на атрибути им овозможуваат на корисниците на дигитален паричник да бараат, да добијат, да складираат и да управуваат со електронски потврди на атрибути.

(2) Давателите на квалификувана доверлива услуга за издавање на електронски потврди на атрибути обезбедуваат интерфејс за издавачите на дигиталните паричници.

Дополнително обезбедување на услугата за издавање на електронска потврда на атрибути

Член 60-ѓ

(1) Давателите на квалификувани и неквалификувани доверливи услуги за електронски потврди на атрибути не смеат да впаруваат или комбинираат лични податоци кои се однесуваат на обезбедувањето на овие услуги со лични податоци од други услуги кои истите ги обезбедуваат директно или од нивни деловни партнери.

(2) Личните податоци кои се поврзани со обезбедување на услуги за електронски потврди на атрибути се чуваат одвоени од другите податоци со кои располага давателот на доверлива услуга за електронски потврди на атрибути.

(3) Давателите на доверлива услуга за издавање на квалификувани електронски потврди на атрибути ја обезбедуваат оваа квалификувана доверлива услуга на начин што е одвоен од сите други услуги што ги обезбедуваат.

11. Електронски записници

Правно дејство на електронски записници

Член 60-е

(1) Не може да се оспорува доказната сила на електронски записник само затоа што е издаден во електронска форма или затоа што не ги исполнува условите за квалификуван електронски записник.

(2) Податоците содржани во квалификуван електронски записник издадени од квалификуван давател на доверлива услуга, се сметаат за потврда на нивниот единствен и точен хронолошки редослед и го задржуваат интегритетот.

Услови што треба да ги исполнат квалификуваните електронски записници

Член 60-ж

(1) Квалификуван електронски записник треба ги исполнува следниве услови:

- да е создадени и управуван од еден или повеќе даватели на квалификувани доверливи услуги,
- да може да се утврди потеклото на записите на податоците во записникот,
- да обезбедува единствено хронолошко подредување на записите со податоци во записникот и
- да ги запишува податоците на таков начин што секоја последователна промена на податоците е веднаш забележлива, со што се обезбедува нивниот интегритет со текот на времето.

(2) Стандардите, спецификации и процедури за исполнување на условите што треба да ги исполнат квалификуваните електронски записници ги пропишува министерот.

VI. ЕЛЕКТРОНСКИ ОВЛАСТУВАЊА

Регистар на овластувања

Член 61

(1) За остварување на права по електронски пат преку полномошник пред секое трето лице, властодавецот може да овласти полномошник преку електронски регистар на овластувања.

(2) Овластувањето се издава со користење на електронска идентификација на властодавецот и со потпишување на овластувањето со квалификуван електронски потпис.

(3) Властодавецот ги определува дејствијата за кои ги издава овластувањето, обемот и рокот на важноста на истото.

(4) Давателот на квалификувана доверлива услуга за издавање на квалификуван сертификат за електронски потпис којшто го издал квалификуваниот сертификат за електронски потпис на властодавецот го води регистарот на овластувања.

(5) Лицата од ставот (4) на овој член го потврдуваат секој запис во регистарот со квалификуван електронски печат и квалификуван електронски временски жиг.

(6) Министерот ја пропишува содржината и начинот на водење на регистарот и проверката на валидноста на овластувањата.

Писмена форма

Член 62

Овластувањата евидентирани во регистарот на овластувања согласно со членот 61 од овој закон имаат иста правна и доказна сила како писмената форма на нотарски заверените овластувања.

Отповикување на овластувањето

Член 63

Отповикувањето на овластувањето се врши со изјава за отповикување на полномошно, дадена на истиот начин и под истите услови како регистрираното овластување.

Водење, чување и пристап до регистарот на овластувања

Член 64

(1) Регистарот на овластувања нема карактер на јавна книга.

(2) Властодателите, овластените лица и засегнатите страни имаат пристап единствено до податоците кои се однесуваат на соодветното овластување поврзано со нив, од Регистарот на овластувања од членот 61 од овој закон.

VII. НАДЗОР И ИНСПЕКЦИСКИ НАДЗОР

Надзор над спроведување на Законот

Член 65

Надзор над спроведувањето на овој закон врши Министерството.

Инспекциски надзор

Член 66

(1) Инспекциски надзор над примената на одредбите од овој закон и другите прописи и општи акти донесени врз основа на овој закон врши секторот надлежен за инспекциски надзор во рамките на Министерството, преку инспекторите за информациско комуникациски технологии (во натамошниот текст: инспекторите).

(2) Инспектори може да бидат вработени лица кои ги исполнуваат условите согласно со Законот за административни службеници и Законот за инспекциски надзор.

(3) При вршењето на инспекцискиот надзор се применуваат одредбите од овој закон, Законот за инспекциски надзор и Законот за општата управна постапка

Опфат на инспекцискиот надзор

Член 66-а

Инспекцискиот надзор над примената на одредбите од овој закон и другите прописи и општи акти донесени врз основа на овој закон опфаќа надзор над:

1) правното дејство на електронските документи;

2) исполнетоста на условите во однос на формата и задолжителните елементи на електронските документи;

3) дигитализација на хартиените документи;

4) исполнетоста на условите на шемите за електронска идентификација;

5) класификацијата на шемите за електронска идентификација;

6) регистрацијата на давателите на доверливи услуги;

7) употребата на шеми за електронска идентификација во електронска трговија и комуникација со јавен орган;

8) исполнетоста на условите за нивоа на сигурност на шеми;

9) исполнетоста на безбедносните услови што треба да ги исполнат издавачите на шемите за електронска идентификација;

10) воспоставеноста на односот меѓу давателот на квалификувана доверлива услуга и корисниците;

11) исполнетоста на условите за обезбедување на квалификувани доверливи услуги од страна на давателите на вакви услуги;

12) исполнувањето на обврската за минималниот износ или видот на покритието на осигурување од ризикот од одговорност за штета причинета од страна на давателот на квалификувана доверлива услуга;

13) верификување на податоците за физичко или правно лице пред издавање на квалификуван сертификат од страна на давателот на квалификувана доверлива услуга;

14) упишувањето на правното лице кое е давател на квалификувана доверлива услуга во Регистарот;

15) исполнетоста на условите на напредниот електронски печат;

16) почитувањето на стандардите кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат;

17) водење и чување на евиденцијата на издадени и укинати сертификати за квалификуван електронски потпис, за електронски печат и за автентичност на веб- страницата;

18) исполнетоста на условите за обезбедување на квалификувана услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат;

19) исполнетоста на условите за обезбедување на квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати;

20) исполнетоста на условите кои треба да ги исполни квалификуваниот електронски временски жиг;

21) исполнетоста на условите за вршење на квалификувана електронска препорачана достава и

22) исполнетоста на условите и стандардите за електронско складирање на документи и за давање на услуга за електронско складирање на документи.

Надлежности и акти на инспекторите

Член 66-б

(1) При вршење на инспекцискиот надзор од членот 66 став (1) од овој закон, инспекторите изрекуваат инспекциски мерки за отстранување на утврдените неправилности и недостатоци во согласност со Законот за инспекциски надзор.

(2) Ако при вршење на инспекцискиот надзор инспекторот утврди неправилности, со решение изрекува опомена и определува рок во кој субјектот на инспекцискиот надзор е должен да ги отстрани неправилностите и недостатоците утврдени со записник.

(3) По исклучок од ставот (2) на овој член, во случај кога инспекторот ќе оцени дека утврдените неправилности и недостатоци можат да предизвикаат или предизвикуваат непосредна опасност по животот и здравјето на луѓето или финансиска штета или штета по имотот од поголема вредност или загрозување на животната средина или загрозување на јавниот интерес, со решение изрекува друга инспекциска мерка од ставот (7) на овој член, со која најсоодветно ќе се постигне целта на инспекцискиот надзор.

(4) Против решението на инспекторите од ставовите (2) и (3) на овој член може да се изјави жалба во рок од 15 дена од денот на приемот на решението до Државната комисија за одлучување во управна постапка, постапка од работен однос и инспекциски надзор во втор степен.

(5) Жалбата изјавена против решението на инспекторите од ставовите (2) и (3) на овој член не го одлага извршувањето на решението.

(6) За изречените опомени од ставот (2) на овој член, инспекторите водат евиденција.

(7) Инспекциските мерки од ставот (1) на овој член опфаќаат:

1) признавање на правно дејство на електронските документи;

2) задолжување за исполнување на условите во однос на формата и задолжителните елементи на електронските документи;

3) задолжување за дигитализација на хартиените документи;

4) забрана за користење на шемите за електронска идентификација кои не ги исполнуваат условите;

5) задолжување за класификацијата на шемите за електронска идентификација;

6) регистрацијата на давателите на доверливи услуги;

7) задолжување за употребата на шеми за електронска идентификација во електронска трговија и комуникација со јавен орган;

8) забрана за издавање и користење на шеми кои не ги исполнуваат законските услови;

9) задолжување за исполнување на безбедносните услови што треба да ги исполнат издавачите на шемите за електронска идентификација и забрана за издавање на шеми до исполнување на тие услови;

10) задолжување за воспоставање на договорен однос меѓу давателот на квалификувана доверлива услуга и корисниците;

11) времена или трајна забрана за вршење на дејност на давателите на квалификувани доверливи услуги кои не ги исполнуваат законските услови;

12) задолжување за полагање на минималниот износ или видот на покритието на осигурување од ризикот од одговорност за штета причинета од страна на давателот на квалификувана доверлива услуга;

13) задолжување за верификување на податоците за физичко или правно лице пред издавање на квалификуван сертификат од страна на давателот на квалификувана доверлива услуга;

14) забрана за вршење на дејност до упишувањето на правното лице кое е давател на квалификувана доверлива услуга во Регистарот;

15) времена или трајна забрана за користење на напредниот електронски печат доколку не ги исполнува законските услови;

16) задолжување за почитување на стандардите кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат и времена или трајна забрана на сертификатите кои не ги исполнуваат овие стандарди;

17) задолжување за водење и чување на евиденцијата на издадени и укинати сертификати за квалификуван електронски потпис, за електронски печат и за автентичност на веб-страницата;

18) времена или трајна забрана за обезбедување на квалификувана услуга за валидација на квалификуван електронски потпис или квалификуван електронски печат доколку не се исполнети условите;

19) времена или трајна забрана за обезбедување на квалификувана доверлива услуга за зачувување на квалификувани електронски потписи или квалификувани електронски печати доколку не се исполнети условите;

20) забрана за издавање и користење на квалификуван електронски временски жиг доколку не се исполнети условите за истиот;

21) забрана за вршење на квалификувана електронска препорачана достава доколку не се исполнети условите за истата и

22) забрана за давање на услуга за електронско складирање на документи и за електронско складирање на документи доколку не се исполнети условите за тоа.

(8) Формата, содржината и начинот на водење на евиденцијата од ставот (6) на овој член ги пропишува министерот.

Прекршочна постапка

Член 66-в

(1) За прекршоците утврдени со овој закон, инспекторот е должен на сторителот на прекршокот да му издаде прекршочен платен налог согласно со Законот за прекршоци пред да поднесе барање за поведување прекршочна постапка пред надлежен суд.

(2) Инспекторот е должен да води евиденција за издадените прекршочни платни налози и за исходот на покренатите постапки.

(3) Во евиденцијата од ставот (2) на овој член, се собираат, обработуваат и чуваат податоците за постапката за издавање на прекршочен платен налог (реден број, број и датум на записник за прекршок и правна квалификација на прекршокот), податоци за сторителот на прекршокот (име и презиме или назив на сторител, адреса/седиште на сторителот и матичен број/ЕДБ на сторителот (за странец се запишува број на патна исправа) и за постапката за извршување (број и датум на платен налог; износ на глоба (во евра); рок за доброволно плаќање на глоба; наплата на глоба (да/не) и датум на поднесено барање за поведување на прекршочна постапка).

(4) Личните податоци од ставот (3) на овој член се чуваат пет години од денот на внесувањето во евиденцијата.

(5) Формата и содржината на прекршочниот платен налог ги пропишува министерот.

(6) За прекршоците утврдени со овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

VIII. ПРЕКРШОЧНИ ОДРЕДБИ

Член 67

(1) Глоба во износ од 5.000 до 10.000 евра во денарска противвредност ќе му се изречат за прекршок на правно лице – давател на квалификувана доверлива услуга, ако:

1) квалификуваните доверливи услуги не ги направи пристапни на лица со попреченост достапни на јасен и разбирлив јазик во согласност со Конвенцијата на Обединетите нации за правата на лицата со попреченост, во согласност со членот 5-а од овој закон;“.

2) не ги преземе потребните технички и организациски мерки за управување со ризиците кои ја загрозуваат сигурноста при обезбедување на доверливи услуги;

3) без одлагање, а најдоцна во рок од 24 часа од моментот на дознавање, не го извести Министерството за секое нарушување на безбедноста или губење на интегритетот, услуги кои имаат значително влијание врз обезбедувањето на доверливите услуги или заштитата на личните податоци кои се обработуваат во рамките на услугите;

4) при нарушување на безбедноста или губење на интегритетот на услугите, без одлагање, не го извести корисникот на доверливите услуги, ако постои закана за безбедност или губење на интегритетот на доверливите услуги или ако може да влијае негативно на корисниците на доверливите услуги;

5) пред склучувањето на договорот од членот 28 став (1) од овој закон не го извести лицето кое го поднело барањето за користење на квалификувани доверливи услуги за сите релевантни околности кои влијаат на услугата согласно со членот 28 став (2) од овој закон;

6) не ги исполнува условите од членот 29 од овој закон;

7) при издавање на квалификувани сертификати за доверливи услуги не ги провери информациите за идентитетот на физичко или правно лице содржани во квалификуваниот сертификат, во согласно со членот 31 став (2) од овој закон;

8) не го известат Министерството најдоцна еден месец пред почетокот на планираната оцена на сообразност, доколку тоа го побара согласно со членот 32 став (8) од овој закон.

9) не ја провери усогласеноста со условите пред започнувањето на обезбедување квалификувани услуги на доверба или најмалку еднаш на секои 24 месеци;

10) пред да започне со вршење на дејноста давател на квалификувана доверлива услуга не е запишан во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација;

11) кој има намера да престане да ја врши оваа дејност е должен за намерата да го извести секој корисник на квалификувани доверливи услуги и Министерството, најдоцна три месеци пред планираниот престанок на вршење на дејноста;

12) во случај на престанок на вршење на дејноста давател на квалификувана доверлива услуга не ги достави сите потребни технички средства во однос на обезбедување на услуги до друг давател на квалификувана доверлива услуга на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги;

13) во случај на престанок на вршење на дејноста давател на квалификувана доверлива услуга не ја достави целокупната документација и опремата во однос на обезбедување на услуги до друг давател на квалификувана доверлива услуга на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги или до Министерството;

14) сертификатите за квалификуван електронски потпис или печат не ги содржат сите податоци наведени во членот 47 став (1) од овој закон;

15) давателот на квалификувана доверлива услуга за издавање на сертификати за квалификуван електронски потпис или печат не ги отповика издадените сертификати во случаите наведени во членот 42 став (1) од овој закон;

16) давателот на квалификувана доверлива услуга за издавање на сертификати за квалификуван електронски потпис или печат не ги извести корисниците на квалификувани доверливи услуги за поништување на сертификатот во рок од 24 часа од приемот на известувањето или појава на околности за кои отповикување сертификат;

17) давателот на квалификувана доверлива услуга за издавање на сертификати за квалификуван електронски потпис или печат не ја зачувува комплетната документација за издадени и одземени сертификати за квалификуван електронски потпис или печат, како и средствата за електронска идентификација и верификација во административни, правни и други процедури, најмалку десет години по истекот на важноста на сертификатот;

18) сигурносното електронско складирање и квалификувано електронско складирање на документи не е спроведено согласно со членот 58 од овој закон.

(2) Глоба во износ од 200 до 500 евра во денарска противвредност ќе му се изрече на одговорно лице во правното лице давател на квалификувана доверлива услуга за прекршоците од ставот (1) на овој член.

(3) Глоба во износ од 5.000 до 10.000 евра во денарска противвредност ќе му се изречат за прекршок на давателот на неквалификувана доверлива услуга ако не го извести Министерството за вршење на дејноста, согласно со членот 24 од овој закон.

(4) Глоба во износ од 200 до 500 евра во денарска противвредност ќе му се изречат за прекршок на одговорното лице во правното лице дavател на неквалификувана доверлива услуга за прекршокот од ставот (3) на овој член.

Член 68

(1) Глоба во износ од 1.000 до 5.000 евра во денарска противвредност ќе му се изречат за прекршок на правно лице корисник на квалификувани доверливи услуги, во случај на промена на податоците наведени во членот 31 став (3) од овој закон, ако не го извести веднаш давателот на квалификувана доверлива услуга.

(2) Глоба во износ од 200 евра до 500 евра во денарска противвредност ќе му се изречат за прекршок на одговорното лице на правното лице корисник на квалификувани доверливи услуги, за прекршокот од ставот (1) на овој член.

(3) Глоба во износ од 100 до 250 евра во денарска противвредност ќе му се изречат за прекршок на физичкото лице корисник на квалификувани доверливи услуги, за прекршокот од ставот (1) на овој член.

Член 69

(1) Глоба во износ од 1.000 до 5.000 евра во денарска противвредност ќе му се изречат за прекршок на правно лице кое има регистрирана шема за електронска идентификација, ако:

1) шемата за електронска идентификација не ја направи пристапна на лица со попреченост, достапна на јасен и разбирлив јазик согласност со Конвенцијата на Обединетите нации за правата на лицата со попреченост, согласност со членот 5-а од овој закон;

2) шемата на електронска идентификација не ги исполнува условите од членот 11 од овој закон;

3) не ги преземе потребните технички и организациски мерки за управување со ризиците кои би можеле да ја нарушат сигурноста и безбедноста при обезбедување на овие услуги согласно со членот 18 од овој закон и

4) не обезбеди технички и организациски мерки заради обезбедување на високо ниво на заштита на личните податоци што може да се користат за прекугранично впарување на идентитетот согласно членот 20-а од овој закон.

(2) Глоба во износ од 200 евра до 500 евра во денарска противвредност ќе му се изречат за прекршок на одговорното лице на правното лице, за прекршокот од ставот (1) на овој член.

Член 70

(1) Глоба во износ од 7.000 до 10.000 евра во денарска противвредност ќе му се изречат за прекршок на правно лице давател на квалификувана доверлива услуга, ако не постапи по наредба на овластеното лице за надзор во рок определен согласно со членот 65 од овој закон.

(2) Глоба во износ од 200 евра до 500 евра во денарска противвредност ќе му се изречат за прекршок на одговорното лице на правното лице давател на квалификувана доверлива услуга, за прекршокот од ставот 1 на овој член.

Член 71

(1) Глоба во износ од 7.000 до 10.000 евра во денарска противвредност ќе му се изречат за прекршок на јавен орган кој нема да ја признае важноста или ќе ја оспори доказната сила на електронскиот документ изготвен согласно со овој закон или дигитализиран документ создаден согласно со членот 10 од овој закон, само затоа што тоа е електронски документ или електронски документ издаден од јавен орган репродуциран на кој било печатен медиум.

(2) Глоба во износ од 200 до 500 евра во денарска противвредност ќе му се изречат за прекршок на функционерот кој раководи со јавниот орган, односно овластеното лице на правното лице кое врши јавни овластувања доколку ја оспорува доказната сила на електронските документи или документите издадени согласно со овој закон, само затоа што се издадени или употребени во електронски формат.

Член 71-а

(1) Глоба во износ од 500 евра до 1.000 евра во денарска противвредност за микро трговци, глоба во износ од 1.000 евра до 2.000 евра во денарска противвредност за мали трговци, глоба во износ од 3.000 евра до 6.000 евра во денарска противвредност за средни трговци и глоба во износ од 5.000 евра до 10.000 евра во денарска противвредност за големи трговци ќе му се изречат за прекршок на правно лице – издавач на дигитален паричник, ако:

1) дигиталниот паричник за крајните корисници не е пристапен на лица со попреченост, достапен на јасен и разбирлив јазик во согласност со Конвенцијата на Обединетите нации за правата на лицата со попреченост согласно членот 5-а од овој закон;

2) не обезбедуваат техничко-технолошки средства и стандарди за валидација согласно со членот 20-д став (4) од овој закон;

3) на своите корисници не обезбедуваат техничка поддршка, која треба да ја добијат при издавање на дигиталниот паричник, вклучително и да пријават технички проблеми или какви било други прекини кои имаат негативно влијание врз употребата на дигиталниот паричник согласно со членот 20-д став (5) од овој закон;

4) не ги обезбедува функционалностите согласно членот 20-ѓ став (1) од овој закон;

5) собира информации за употребата на дигиталниот паричник што не се неопходни за обезбедување на услугите на дигиталниот паричник, или комбинира, односно впарува податоци за идентификација на лица или какви било други лични податоци складирани или поврзани со употребата на дигиталниот паричник со лични податоци од кои било други услуги кои ги обезбедува издавачот на дигиталниот паричник, освен ако корисникот изречно не побарал поинаку спротивно на членот 20-ж став (2) од овој закон;

6) техничките правила кои се имплементираат за издавање и користење на дигиталниот паричник, односно техничката рамка за дигитален паричник не овозможуваат на давателите електронски потврди на атрибути или на која било друга страна, по издавањето на електронските потврди на атрибутите, да добиваат податоци што овозможуваат следење, поврзување или впарување на трансакциите или однесувањето на корисникот на дигитален паричник или да се добијат податоци за постоење за трансакциите или однесувањето на корисникот, освен ако корисникот не дал согласност за таква обработка на наведените податоци спротивно на членот 20-з став (1) точка (а) од овој закон;

7) техничките правила кои се имплементираат за издавање и користење на дигиталниот паричник, односно техничката рамка за дигитален паричник не овозможуваат имплементација на техники за зачувување на приватноста кои обезбедуваат неповрзаност на податоци, каде што потврдувањето на атрибутите не бара идентификација на корисникот спротивно на членот 20-з став (1) точка (б) од овој закон;

8) пред издавањето на дигиталните паричници, издавачите на дигитални паричници поднесуваат барање, доставуваат податоци и документи до Министерството заради упис во Листата на сертифицирани дигитални паричници согласно членот 20-ј став (1) од овој закон;

9) во случај на промена на податоците содржани во листата за сертифицирани дигитални паричници, издавачот на дигитален паричник не доставува ажурирани податоци или документи до Министерството во рок од 15 дена од денот на настанувањето на промената согласно членот 20-ј став (4) од овој закон;

10) во случаите кога е нарушена безбедноста на дигиталните паричници, техничко-технолошки средства и стандарди за валидација или шемата за електронска идентификација според која се обезбедуваат дигиталните паричници на начин што влијае на нивната веродостојност или на веродостојноста на други дигитални паричници, веднаш не го суспендира обезбедувањето и користењето на дигиталните паричници спротивно на членот 20-к став (1) од овој закон;

11) во случаите кога е нарушена безбедноста на дигиталните паричници, техничко-технолошки средства и стандарди за валидација или шемата за електронска идентификација според која се обезбедуваат дигиталните паричници на начин што влијае на нивната веродостојност или на веродостојноста на други дигитални паричници, соодветно не ги информира корисниците на дигиталниот паричник, засегнатите страни и Министерството, спротивно на членот 20-к став (3) од овој закон;

12) во случаите кога е нарушена безбедноста на дигиталните паричници, техничко-технолошки средства и стандарди за валидација или шемата за електронска идентификација според која се обезбедуваат дигиталните паричници на начин што влијае на нивната веродостојност или на веродостојноста на други дигитални паричници веднаш, но не подоцна од 72 часа од настанувањето на нарушувањето на безбедноста или компромитирањето не го Министерството согласно со членот 20-к став (4) од овој закон;

13) во случаите кога од нарушувањето на безбедноста се засегнати лични податоци, веднаш, но не подоцна од 72 часа од настанувањето на нарушувањето на безбедноста или компромитирањето не ја информира Агенцијата за заштита на личните податоци и соодветно не ја информира јавноста согласно со членот 20-к став (5) од овој закон;

(2) Глоба во износ од 150 до 250 евра во денарска противвредност ќе му се изрече на одговорно лице во правното лице издавач на дигитален паричник за прекршоците од ставот (1) на овој член.

Член 71-б

(1) Глоба во износ од 150 до 250 евра во денарска противвредност ќе му се изрече за прекршок на физичкото лице корисник на дигиталниот паричник, ако:

1) не да ги чува средствата и податоците за издавање на електронски потпис или печат од неовластен пристап и користење и истите не ги користи во согласност со одредбите на овој закон согласно со членот 20-љ став (1) од овој закон или

2) не ги чува средствата и податоците за издавање на дигиталниот паричник од неовластен пристап и користење и не го користи во согласност со одредбите на овој закон согласно со членот 20-љ став (2) од овој закон.

Член 71-в

(1) Глоба во износ од 500 евра до 1.000 евра во денарска противвредност за микро трговци, глоба во износ од 1.000 евра до 2.000 евра во денарска противвредност за мали трговци, глоба во износ од 3.000 евра до 6.000 евра во денарска противвредност за средни трговци и глоба во износ од 5.000 евра до 10.000 евра во денарска противвредност за големи трговци ќе му се изрече за прекршок на правно лице – засегната страна, ако:

1) не го извести Министерството за намерата да овозможи употреба на дигитален паричник за обезбедување на електронска услуга согласно со членот 20-ѕ став (1) од овој закон;

2) бара од корисниците други податоци, освен оние кои се определени во членот 20-ѕ став (2) од овој закон, спротивно на членот 20-ѕ став (3) од овој закон;

3) без одлагање не го извести Министерството за секоја измена на податоците кои се содржани во Регистарот спротивно на членот 20-ѕ став (5) од овој закон и

4) не се идентификува пред корисникот согласно со членот 20-ѕ став (6) од овој закон.

(2) Глоба во износ од 150 до 250 евра во денарска противвредност ќе му се изрече на одговорното лице во правното лице засегната страна за прекршоците од ставот (1) на овој член.

Член 72

(1) За прекршоците утврдени со овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

IX. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 73

Подзаконските акти чие донесување е утврдено со овој закон ќе се донесат во рок од три месеци од денот на влегувањето во сила на овој закон.

Член 74

1) Електронските потписи, електронските печати и електронските временски жигови издадени до денот на започнувањето на примената на овој закон согласно со Законот за податоците во електронски облик и електронски потпис, продолжуваат да важат се до истекот на нивната важност.

(2) Правните лица кои вршат дејност до денот на започнувањето на примената на овој закон согласно со Законот за податоците во електронски облик и електронски потпис, со влегувањето во сила на овој закон ќе продолжат да ги издаваат електронските потписи и ќе ги обезбедуваат услугите согласно со Законот за податоците во електронски облик и електронски потпис.

Член 75

(1) Давателите на доверлива услуга, односно издавачите на сертификати кои вршат дејност врз основа на Законот за податоците во електронски облик и електронски потпис се должни да го усогласат своето работење со одредбите на овој закон најдоцна до 1 септември 2020 година.

(2) Во периодот до усогласување со одредбите на овој закон, давателите на доверлива услуга од ставот (1) на овој член, односно издавачите на сертификати ги обезбедуваат услугите за издавање на сертификати за електронски потписи, електронски печати и временски жигови согласно со Законот за податоците во електронски облик и електронски потпис.

(3) Давателите на доверлива услуга кои вршат дејност врз основа на Законот за податоците во електронски облик и електронски потпис, а кои нема да го усогласат своето работење во рок од една година од денот на донесувањето на подзаконските акти предвидени со овој закон нема да бидат запишани во Регистарот за шеми за електронска идентификација и за доверливи услуги.

Член 76

Овој закон престанува да важи со пристапувањето на Република Северна Македонија во Европската Унија.

Член 77

Со денот на започнувањето на примената на овој закон престанува да важи Законот за податоците во електронски облик и електронски потпис („Службен весник на Република Македонија" број 34/2001, 6/2002, 98/2008 и 33/15).

Член 78

Овој закон влегува во сила со денот на објавувањето во „Службен весник на Република Северна Македонија", а ќе започне да се применува од 1 септември 2020 година, освен одредбите од глава II. Електронски документ кои ќе започнат да се применуваат од 20 декември 2019 година.

ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ
од Законот за изменување и дополнување
на Законот за електронски документи,
електронска идентификација и доверливи услуги
("Службен весник на РСМ" бр. 275/19)

Член 7

Правилникот определен со членот 1 од овој закон ќе се донесе најдоцна до денот на влегувањето во сила на овој закон.

Член 8

Овој закон влегува во сила со денот на објавувањето во „Службен весник на Република Северна Македонија".

ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ
од Законот за изменување и дополнување
на Законот за електронски документи,
електронска идентификација и доверливи услуги
("Службен весник на РСМ" бр.3/25)

Член 41

Подзаконските акти кои произлегуваат од овој закон ќе се донесат во рок од 90 дена од денот на влегувањето во сила на овој закон.

Член 42

Овој закон влегува во сила со денот на објавувањето во „Службен весник на Република Северна Македонија".

ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ од Законот за изменување и дополнување на Законот за електронски документи, електронска идентификација и доверливи услуги ("Службен весник на РСМ" бр.135/25)

Член 23

(1) Давателите на доверливи услуги и издавачите на шеми за електронска идентификација кои се регистрирани во Регистарот на на даватели на доверливи услуги и на шеми за електронска идентификација, во согласност со Законот за електронски документи, електронска идентификација и доверливи услуги („Службен весник на Република Северна Македонија" број 101/19, 275/19 и 3/25), се должни да го усогласат своето работење со одредбите од овој закон кои се однесуваат на доверливи услуги и на шеми за електронска идентификација во рок од 12 месеци од денот на влегувањето во сила на овој закон.

(2) Електронските потписи, електронските печати и електронските временски жигови издадени до денот на започнување со примена на овој закон, продолжуваат да важат сè до истекот на нивната важност.

Член 24

Започнатите постапки до денот на започнување со примена на овој закон, ќе завршат согласно со Законот за електронски документи, електронска идентификација и доверливи услуги („Службен весник на Република Северна Македонија" број 101/19, 275/19 и 3/25).

Член 25

Подзаконските акти предвидени со овој закон ќе се донесат во рок од шест месеци од денот на влегувањето во сила на овој закон.

Член 26

Овој закон престанува да важи со пристапувањето на Република Северна Македонија во Европската Унија.

Член 27

Овој закон влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија", а ќе започне да се применува од 1 јуни 2027 година.