

ЗАКОН ЗА ЕЛЕКТРОНСКИ ДОКУМЕНТИ, ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА И ДОВЕРЛИВИ УСЛУГИ

I. ОПШТИ ОДРЕДБИ

Предмет

Член 1

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

Со овој закон се утврдува и начинот на употреба на електронските документи, електронскиот потпис и електронскиот печат и електронските доверливи услуги во управни и судски постапки.

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

Целта на овој закон е да се обезбеди соодветно ниво на безбедност на средствата за електронска идентификација и соодветно ниво на безбедност при обезбедување доверливи услуги.

Цел на овој закон е да се утврди правниот режим на електронските потписи, електронските печати, електронските временски жигови, електронските документи, услугите за електронска препорачана достава, услугите за проверка на автентичност на веб страници, како и начинот на чување на електронскиот потпис или печат и нивна валидација.

Дефиниции

Член 3

Изразите употребени во овој закон, го имаат следново значење:

- 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 секој документ складиран во електронска форма, особено текстуални или звучни, визуелни или аудио-визуелни записи;
- 4) **производ** значи хардвер, софтвер или соодветните компоненти на хардвер или софтвер предвидени да се користат при обезбедување на доверливи услуги;
- 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 поединци на кои им се делегирани јавни овластувања во согласност со законодавството на Република Македонија или законодавството на Европската унија;

- 7) **автентикација** значи електронски процес кој овозможува 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 идентитетот на правно лице, физичко лице или овластено лице на правно лице;
- 9) **електронска идентификација** претставува процес на користење на податоци за идентификација на лица во електронска форма кои на уникатен начин го претставуваат физичкото или правно лице или овластено лице на правно лице;
- 10) **средства за електронска идентификација** се материјални или нематеријални средства кои содржат податоци за идентификација на лица, а се користат за автентикација кај електронски услуги;
- 11) **издавач на средство за електронска идентификација** е правно лице давател на доверливи услуги, во согласност со условите пропишани во овој закон за издавачи на средство за електронска идентификација;
- 12) **шема за електронска идентификација** значи систем за електронска идентификација според кој средствата за електронска идентификација се издаваат на физички или правни лица или овластено лице на правно лице;
- 13) **доверлива услуга** значи електронска услуга која се состои од:
- создавање, валидација и верификација на електронски потписи, електронски печати или електронски временски жигови, услуги за електронска препорачана достава, како и сертификати поврзани со овие услуги или
 - создавање, валидација и верификација на сертификати за автентичност на веб страници или
 - чување на електронски потписи, печати или потврди поврзани со овие услуги.
- Доверливите услуги може да бидат неквалификувани и квалификувани.
- 14) **давател на доверливи услуги** значи физичко или правно лице кое обезбедува една или повеќе доверливи услуги;
- 15) **засегната страна** во смисла на овој закон значи физичко или правно лице кое има правен интерес од електронска идентификација или доверливи услуги;
- 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** значи давател на доверлива услуга кој обезбедува една или повеќе квалификувани доверливи услуги и чиј статус на квалификуван давател на доверлива услуга е доделен од страна на министерот за информатичко општество и администрација со регистрација во Регистарот. Давателот на квалификувана доверлива услуга е лице на кое му се доделени јавни овластувања, согласно 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) **овластен управувач со електронски печат** е овластено лице на правно лице кое создава електронски печат;
- 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 електронскиот потпис или електронскиот печат се валидни;
- 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** значи 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 пропишани со овој закон, а кои се однесуваат на средства за создавање на квалификуван електронски потпис или печат;
- 31) **квалификуван сертификат за електронски потпис** е потврда за електронски потпис издадена од давател на квалификувани доверливи услуги и која ги исполнува условите пропишани со овој закон, а кои се однесуваат на квалификуван сертификат за електронски потпис;
- 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 напреден 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 овластениот управувач со електронски печат за создавање на електронски печат;
- 35) **квалификуван сертификат за електронски печат** е потврда за електронски печат издаден од давател на квалификувани доверливи услуги и ги исполнува условите пропишани со 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 потврда за автентикација на веб страница издадена од давател на квалификувани доверливи услуги и ги исполнува условите пропишани со 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 пропишани со 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 недозволените измени;
- 41) **квалификувана електронска препорачана достава** е услуга за електронска препорачана достава што ги исполнува условите пропишани со 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** означува чување на документи во електронска форма, за кои е точно определено времето на чување на тие документи, соодветно на времето на чување на документите во печатена форма, за кои времето на складирање е потврдено со електронски временски жиг;
- 46) **квалификувано електронско складирање на документи** означува чување на електронски документи, кои при нивното складирање се потврдени со квалификуван електронски потпис или печат и квалификуван временски жиг;
- 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 доверливи услуги;
- 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 квалификувани доверливи услуги;
- 49) **тело за оценување на сообразноста** е правно лице акредитирано да врши проценка на усогласеноста на квалификуваниот давател на доверливи услуги и на квалификуваните доверливи услуги кои истиот ги обезбедува;
- 50) **лабораторија за сертификација** е правно лице акредитирано да врши проценка на усогласеност на средствата за издавање на електронска идентификација, електронски потписи или електронски печати.

Примена на законот

Член 4

Давателот на доверливи услуги ги обезбедува доверливите услуги во согласност со одредбите од овој закон.

Одредбите од овој закон не се применуваат на доверливи услуги што се обезбедуваат 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.

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 утврдени во Регулативата бр. 910/2014 на Европскиот парламент и на Советот (eIDAS) или кој било друг безбеден, далечински или електронски процес на идентификација регулиран, признат, одобрен или прифатен од релевантните национални органи или од органите на земја членка на Европската унија.

Обработка и заштита на лични податоци

Член 5

Давателот на доверливи услуги при обработката на личните податоци до кои има пристап во текот на вршењето на дејноста постапува согласно со прописите со кои се уредува заштитата на личните податоци.

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.

II. ЕЛЕКТРОНСКИ ДОКУМЕНТ

Правно дејство на електронскиот документ

Член 6

Електронскиот документ има иста правна и доказна сила како и писмената форма на документот, во согласност со закон.

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

Кога со закон е пропишана писмена форма на документите или актите, електронскиот документ се смета за документ или акт во писмена форма.

Создавање на електронски документ

Член 7

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

Електронскиот документ како архивски материјал се создава во форма која ги исполнува условите пропишани со овој закон, а е погодна за сигурносна подготовка за електронско складирање.

Оригинал и копија

Член 8

Секој умножен примерок на електронскиот документ се смета за оригинал.

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

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

Дигитализација на документи

Член 9

Дигитализираниот документ ја има истата правна и доказна сила како оригиналниот документ, доколку кумулативно се исполнети условите од точка 1) и точка 2) на овој став и тоа:

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

- физичко лице или овластено лице на правно лице кој што 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, во согласност со прописите што го уредуваат архивското и канцелариското работење или
- лица кои се овластени со овој или друг закон да го потврдат дигитализираниот документ и

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

Верификација на печатена форма на електронски документ

Член 10

Електронскиот документ репродуциран на било кој печатен медиум ја има истата правна и доказна сила како оригиналниот електронски документ, доколку кумулативно се исполнети условите од точка 1) и точка 2) на овој став и тоа:

- 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.

III. ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

1. Шеми за електронска идентификација

Услови кои треба да ги исполнуваат шемите за електронска идентификација

Член 11

Шемите за електронска идентификација задолжително треба да 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, определени со член 13 од овој закон.

Согласност за идентификација

Член 12

Постапката за издавање на електронска идентификација може да се поведе само по претходно барање на физичко или правно лице кое е субјект на идентификација, освен ако со закон поинаку не е определено.

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;
- 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

Давателот на доверливи услуги до министерството за информатичко општество и администрација 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 за информатичко општество и администрација. Во Регистарот задолжително се регистрираат шемите за електронска идентификација кои ги употребуваат јавните органи.

Во Регистарот може да се регистрираат и шеми за електронска идентификација кои се создадени од јавни органи и шеми кои се создадени од приватни правни лица.

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

Шемите создадени од приватни правни лица задолжително треба да одговараат на високо ниво за сигурност за да бидат регистрираат во Регистарот.

Регистарот од став 1 на овој член ги содржи следните информации за давателот на доверливи услуги:

- име на правното лице,
- информации за контакт како што се: адреса, телефонски број и електронска пошта;
- видот на услуги што ги обезбедува издавачотна шемата за електронска идентификација

- средствата за електронска идентификација кои се користат во рамки на шемата
- нивото на сигурност.

Во Регистарот се регистрираат и давателите на квалификувани доверливи услуги. Министерот за информатичко општество и администрација 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

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 на овој закон (во натамошниот текст: регистрирана шема за електронска идентификација).

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

Одговорност за штета од употреба на регистрирани шеми за електронска идентификација

Член 16

Издавачот на регистрирана шема за електронска идентификација е одговорен за штетата која може да настане поради тоа што шемата не ги исполнува условите од членот 18 на овој закон.

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.

Товарот за докажување за настаната штета е на страна на лицето што истакнало побарување за надомест на штета.

Издавачот задолжително треба да е осигуран од професионална одговорност или да има обезбедени финансиски средства како задолжително финансиско покритие.

Износот на финансиските средства кои треба да бидат обезбедени за оваа намена или нивото на покритие за штети предизвикани од професионална одговорност го утврдува министерот за информатичко општество и администрација.

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

Член 17

Барањето за утврдување на исполнетост на услови за нивоа на сигурност на шеми е прилог кон барањето за регистрација во Регистарот.

Барањето ги содржи следните податоци:

- 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 оценка на сообразност 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

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.

Техничките 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.

Условите кои треба да ги исполнат техничките и организациски мерки за сигурност на шеми за електронска идентификација ги пропишува министерот за информатичко општество и администрација.

Оценката на нивото на сигурност на шемата за електронска идентификација ја оценува телото за сообразност кое е акредитирано да врши сертификација по меѓународни стандарди, определени во соодветен подзаконски акт утврден во ставот 3 на овој член.

2. Прекугранична соработка во областа на електронската идентификација

Интероперабилност на техничките системи

Член 19

Министерството за информатичко општество и администрација соработува со релевантни меѓународни тела 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 признаените шеми за електронска идентификација.

Регистрација на шеми за електронска идентификација

издадени од странски правни лица

Член 20

Министерството за информатичко општество и администрација може да регистрира во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација и странски правни лица кои ги исполнуваат барањата од Регулативата на ЕУ бр. 910/2014 на Европскиот парламент и на Советот (во натамошниот текст: регулатива eIDAS).

Министерството за информатичко општество и администрација 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.

IV. ДОВЕРЛИВИ УСЛУГИ

1. Општи одредби за доверливи услуги

Вид на доверливи услуги

Член 21

Доверливи услуги се услугите кои се определени како доверливи во согласност со одредбите од овој закон.

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 автентикација на веб страници,
- 4) квалификувана доверлива услуга на чување на квалификувани електронски потписи,
- 5) квалификувана доверлива услуга на чување на квалификувани електронски печат,
- 6) квалификувана валидација на квалификуван електронски потпис,
- 7) квалификувана валидација на квалификуван електронски печат,
- 8) квалификувана доверлива услуга на издавање квалификувани електронски временски печат,
- 9) квалификувана доверлива услуга на електронска препорачана достава и
- 10) квалификувана доверлива услуга за електронско складирање на документи.

Давателот на доверливи услуги или давателот на квалификувани доверливи услуги може да обезбеди една или повеќе услуги наведени во ставовите 1 и 2 на овој член.

Одговорност на давателите на доверливи услуги

Член 22

Давател на доверливи услуги е одговорен за штетата која настанала како последица од непостапување во согласност со овој закон, ако штетата е предизвикана намерно или од небрежност.

Товарот за докажување на намерата или небрежноста на давател на доверливи услуги е на физичко или правно лице кое бара надомест на штета од став 1 на овој член.

Кога давателите на доверливи услуги 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.

Давателот на квалификувани доверливи услуги треба да биде осигуран од штета или да обезбеди финансиски средства на начин и под услови 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

Давателот на неквалификувани доверливи услуги, е должен да го извести министерството за информатичко општество и администрација за вршење на дејност најдоцна во рок од 15 дена сметано од денот на започнувањето на вршење на дејноста. Давателот на неквалификувани доверливи услуги 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.

Министерството за информатичко општество и администрација ги запишува услугите во Регистарот, врз основа на поднесеното известување доколку истото е целосно.

Давател на квалификувани доверливи услуги пред да започне да ја врши својата дејност е должен да поднесе барање за регистрација во Регистарот.

Давателите на доверливи услуги се должни да ги преземат потребните технички и организациски мерки за управување со ризици кои би можеле да ја загрозат сигурноста при обезбедување на овие услуги.

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.

Давателите на доверливи услуги, без одлагање и најдоцна во рок од 24 часа од моментот на дознавањето, ќе го известат надлежниот орган за какви било нарушувања на безбедноста или намалување на интегритетот на услугата кои имаат значително влијание врз обезбедувањето доверливите услуги или заштитата на личните податоци кои се обработуваат во рамките на обезбедувањето на услугата.

Во случај кога нарушувањето на безбедноста е поврзано со заштитата на личните податоци, давателот на доверливи услуги ја известува и Дирекцијата за заштита на личните податоци.

Доколку нарушувањето на безбедноста или губење на интегритетот на доверливата услуга може негативно да влијае на корисниците на доверливите услуги, давателот на доверливи услуги должен без одлагање да го информира корисникот на доверливата услуга.

Надлежниот орган ја информира јавноста доколку утврди дека со нарушувањето на безбедноста или губењето на интегритетот на доверливите услуги е засегнат јавниот интерес.

Надлежниот орган соработува со релевантни институции од други земји во врска со размена на информации за безбедноста и интегритетот на доверливите услуги, во согласност со ратификуваните меѓународни договори.

Надлежност на министерството за информатичко општество и администрација

Член 25

Министерството за информатичко општество и администрација 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 квалификувани доверливи услуги;
- 3) врши инспекциски надзор над работата на давателите на доверливи услуги и издавачите на шеми за електронска идентификација;
- 4) иницира надзор пред тело за сообразност;
- 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 доверливи услуги, 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 наведени во член 17 од регулативата на eIDAS;
- 9) ги пропишува подзаконските акти определени со овој закон.

Надлежности на министерството за информатичко општество и администрација во рамки на прекугранична соработка

Член 26

Министерството за информатичко општество и администрација во рамки на прекуграничната соработка доставува извештаи до Европската комисија за своите активности во согласност со регулативата eIDAS, почнувајќи од датумот на пристапување на Република Македонија во Европската унија.

Надлежен орган за акредитација

Член 27

Национален орган за акредитација на телата за оцена на сообразност и лабораториите за сертификација на средствата определени со овој закон е Националниот институт за акредитација, согласно Законот за акредитација.

Националниот институт за акредитација донесува методологија за акредитација на тела за оцена на сообразност и лаборатории за сертификација на средства врз основа на стандардите определени од страна на министерот за информатичко општество и администрација.

Министерството за информатичко општество и администрација води листа на акредитирани тела за сообразност и лаборатории.

Акредитацијата извршена од страна на надлежен орган за акредитација од земја членка на Европската унија се смета за акредитација извршена во Република Македонија.

2. Општи одредби за квалификувани доверливи услуги

Воспоставување на односот помеѓу давателот на квалификувани доверливи услуги и корисниците

Член 28

Квалификувана доверлива услуга се обезбедува врз основа на склучен договор помеѓу давателот на квалификувани доверливи услуги и корисникот на истите, кој договор се склучува по претходно барање од корисникот.

Давателот на квалификувани доверливи услуги, пред склучување на договорот од став 1 на овој член, на јасен и недвосмислен 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;
- 3) мерките што треба да ги преземе корисникот на квалификуваните доверливи услуги и потребната технологија за безбедно користење на квалификувана доверлива услуга.

Услови за обезбедување на квалификувани доверливи услуги

Член 29

Давателот на квалификувани доверливи услуги треба да ги исполни следните услови и тоа:

- 1) да има вработено или ангажирано 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 соодветна обука во областа на информатичката безбедност;
- 2) да биде осигуран од професионална одговорност за штета или да има обезбедено финансиски средства за надомест 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 квалификувани доверливи услуги, 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;
- 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 Македонија.

Давателот на квалификувани доверливи услуги 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 квалификувани доверливи услуги ги користи за да се обезбеди давање на услуги во согласност со прописите и општите услови наведени во точка 1) од овој став.

Услов за вршење на дејноста квалификуван давател на доверливи услуги е уписот во Регистарот на доверливи услуги и шеми за електронска идентификација.

Осигурување од професионална одговорност

Член 30

Министерот за информатичко општество и администрација го пропишува минималниот износ или видот на покритието на осигурување од ризикот од одговорност за штета причинета од страна на давател на квалификувани доверливи услуги.

Идентификација на корисникот на квалификувани доверливи услуги

Член 31

Давателот на квалификувани доверливи услуги ги верификува податоците за физичко или правно лице пред издавање на квалификуван сертификат, во согласност со закон. Проверката на податоците од ставот 1 на овој член давателот на квалификувани доверливи услуги 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 член 13 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); 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 оценка на сообразноста го потврдува еднаквото ниво на сигурност.
- 5) со начин за идентификација, употребен во земја членка на Европската унија во согласност со одредбите на регулативата eIDAS.

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 7 дена да го извести давателот на квалификуваната доверлива услуги за настанатата промена.

За идентификација и користење на квалификувани доверливи услуги, давателот на квалификувани доверливи услуги и издавачот на шеми за електронска идентификација може изврши верификација 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

Оценување на исполнетоста на условите за обезбедување на квалификувани доверливи услуги врши тело за оценка на сообразност.

Тело за оценување на сообразноста е правно лице акредитирано да врши проценка на усогласеноста на квалификуваниот давател на доверливи услуги и квалификуваните доверливи услуги кои истиот ги обезбедува.

Телото за оценување на сообразноста е надлежно и за вршење на проверка на сообразност и за неквалификувани даватели на доверливи услуги, по претходна иницијатива на министерството за информатичко општество и администрација или по барање на давателот на услугата.

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

Оценувањето за сообразност задолжително се врши пред почетокот на вршење на дејноста давател на квалификувани доверливи услуги, како и најмалку еднаш на секои 24 месеци, за секој давател на квалификувани доверливи услуги.

По изготвениот извештај за спроведената оцена на сообразност на барателот или давателот на квалификувани доверливи услуги, телото за оцена на сообразност извештајот го доставува до министерството за информатичко општество и администрација, во рок од три работни дена од денот кога истиот е завршен.

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 информаците.

Цената на оценување на сообразност, вклучувајќи преоценка за итни случаи, се на товар на давателот на квалификувани доверливи услуги.

Министерот за информатичко општество и администрација утврдува листа на стандарди кои треба да бидат исполнети од страна на телото за оцена 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 Македонија или во земја членка на Европската унија да вршат оцена на сообразност.

Постапка за упис на давател на квалификувани доверливи услуги во Регистарот

Член 33

Давателот на квалификувани доверливи услуги поднесува барање до министерството за информатичко општество и администрација за регистрација во Регистарот, пред да започне да врши дејност давател на квалификувани доверливи услуги.

Во прилог на барањето од ставот 1 на овој член се приложуваат и докази за фактите наведени во барањето, вклучувајќи го и извештајот за оцена на сообразност во согласност со член 32 од овој закон.

Министерството за информатичко општество и администрација донесува решение за регистрација на барателот во Регистарот, со кое на давателот на доверливи услуги му доделува статус на квалификуван давател на доверливи услуги, во рок од 60 дена од денот на приемот на барањето, доколку истото е целосно и во зависност од наводите од извештајот за оцена на сообразност.

По исклучок, доколку се работи за дополнителни проверки или прибавување на дополнителни докази за кои е потребен подолг рок, министерството за информатичко општество и администрација ќе го пролжи рокот на начин и под услови утврдени со закон.

При одлучувањето, министерството за информатичко општество и администрација 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. Доколку барателот или услугите наведени во барањето не ги исполнуваат условите пропишани со овој закон, министерството за информатичко општество и администрација донесува решение за отфрлање на барањето за регистрација во регистарот.

Престанок на вршење на дејноста давател на квалификувани доверливи услуги

Член 34

Давателот на квалификувани доверливи услуги кој има намера да престане да ја врши оваа дејност е должен за намерата да ги извести корисниците на квалификувани доверливи услуги и министерството за информатичко општество и администрација, најдоцна три месеци пред планираниот престанок на вршење на дејноста.

Давателот на квалификувани доверливи услуги кој ќе престане да ја врши оваа дејност е должен да обезбеди друг давател на квалификувани доверливи услуги кој ќе продолжи со извршувањето на овие услуги за корисниците на квалификуваните доверливи услуги, и за преземените мерки веднаш ќе го извести министерството за информатичко општество и администрација.

Давателот на квалификувани доверливи услуги 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 квалификувани доверливи услуги на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги.

Доколку давателот на квалификувани доверливи услуги не постапи во согласност со обврската утврдена во став 2 и став 3 на овој член, министерството за информатичко општество и администрација ќе побара од давателот на квалификувани доверливи услуги без одлагање до министерството да ја достави целокупната документација и опрема, вклучително и процедурите за постапување со истите.

Министерството привремено ќе ја чува документацијата, сè до обезбедување на друг давател на квалификувани доверливи услуги кој ќе продолжи да ги извршува овие услуги за корисниците, за сметка на давателот на квалификувани доверливи услуги кој престанува да ја врши оваа дејност.

За начинот на чување на документацијата и условите под кои министерството ќе ја чува истата, министерот за информатичко општество и администрација ќе донесе посебен правилник.

Во случај на привремена забрана за вршење на дејност давател на квалификувани 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

Министерството за информатичко општество и администрација објавува листа на даватели на квалификувани доверливи услуги, како и листа на квалификувани доверливи услуги кои тие ги обезбедуваат, во електронска форма која е погодна за автоматска обработка.

Листата од ставот 1 на овој член е потпишана или печатирана со електронски потпис или печат на министерството за информатичко општество и администрација.

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. Формата и начинот на објавување на листата од ставот 1 на овој член, треба да бидат во согласност со техничките барања за листата на доверба во согласност со член 22 од Регулативата 910/2014 на ЕУ.

Ознака за доверба на квалификувани доверливи услуги

Член 36

Ознаката за доверба на квалификувана доверлива услуга (во понатамошниот текст како ознака за доверба) е знак кој е едноставен, препознатлив и јасно укажува на квалификувана доверлива услуга.

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 даватели на квалификувани доверливи услуги

Министерот за информатичко општество и администрација ги пропишува формата, структурата, големината и логото на ознаката за доверба на квалификувани доверливи услуги.

Прекугранично признавање на даватели на доверливи услуги

Член 37

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

Давателите на доверливи услуги основани и се под надзор на земја членка на Европската Унија и кои се запишани во Листата на ЕУ, можат да работат и да обезбедуваат услуги на територијата на Република Македонија, без претходна регистрација во Регистарот на даватели на доверливи услуги и шеми за електронска идентификација.

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 да ги исполнува следните услови:

- 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) 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 да ги исполнува следните услови:

- 1) да биде на единствен начин поврзан со управувачот со печатот,

- 2) да овозможи идентификација на управувачот со печатот,
- 3) да е создаден со податоци за создавање на електронски печат кои управувачот со печатот, со високо ниво на доверба, може да ги користи за создавање на електронски печат
- 4) е поврзан со податоците кои ги печатира на таков начин што секоја подоцнежна измена на истите е воочлива.

3. Содржина на квалификуван сертификат за електронски потпис и печат

Член 40

Стандардите кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат ги пропишува министерот за информатичко општество и администрација со правилник.

Покрај стандардите кои треба да ги содржат квалификуваните сертификати за електронски потпис и за електронски печат, можат да содржат и дополнителни елементи кои нема да имаат влијание врз интероперабилноста и признавањето на квалификуваниот електронски потпис.

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

Член 41

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

Поништување или суспензија на квалификуван сертификат за електронски потпис или печат

Член 42

Давателот на доверливи услуги кој го издава квалификуваниот сертификат за електронски потпис или печат е должен да го отповика издадениот квалификуван сертификат, доколку:

- 1) сопственикот на сертификатот за квалификуван електронски потпис или печат 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 или печат или системот на давателот на квалификувани доверливи услуги е компромитиран на начин кој влијае врз безбедноста и сигурноста на сертификатите;
- 5) утврди дека податоците за создавање на електронски потпис или печат или системот преку кој се извршува електронска трансакција се изложени на ризик, на начин кој влијае на сигурноста и безбедноста на електронскиот потпис или печат;
- 6) настане престанок на правно лице, на начин и под услови утврдени со закон.

Давателот на доверливи услуги кој го издава квалификуваниот сертификат за електронски потпис или печат го известува корисникот на квалификуваните доверливи услуги 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.

Корисникот на квалификувани доверливи услуги е должен да побара поништување на издадениот сертификат за квалификуван електронски потпис или печат во случај на

губење, оштетување или загрозување на интегритетот на податоците од сертификатот, или доколку настане промена на податоците за креирање сертификати.

Во случај на суспензија на сертификат за квалификуван електронски потпис или печат истиот губи важност за времетраење на периодот на важноста на суспензијата.

Информациите за суспензија и нејзиното времетраењеквалификуван сертификат за електронски потпис или печат ќе бидат внесени во базата на податоци на издадени квалификувани сертификати кои се чуваат од страна на давателот на квалификувани доверливи услуги, и истите ќе бидат видливи при проверка статусот на валидност на квалификуван електронски сертификат.

Евиденција на издадени и одземени сертификати за квалификуван електронски потпис или печат

Член 43

Издавачот на сертификати за квалификувани сертификати за електронски потпис или печат е должен да ја чува целокупната документација за издадени и одземени квалификуваните сертификати за електронски потпис или печат, 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 одземање.

Податоците од ставот 1 на овој член може да се чуваат во електронска форма.

Средства за создавање на квалификуван електронски потпис или квалификуван електронски печат

Член 44

Министерот за информатичко општество и администрација ги пропишува техничките услови кои треба да бидат исполнети и начинот на создавање на квалификувани електронски потписи или печати од страна на давателите на квалификувани доверливи услуги со правилник.

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

Член 45

Оцена на исполнетост на техничките услови што се однесуваат на средствата за издавање на квалификувани електронски потписи и печати врши акредитирана лабораторија.

Лабораторијата издава потврда за сообразност на средство за создавање на квалификувани електронски потписи и квалификувани електронски печати.

Техничките услови и 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 член 44 од овој закон.

Министерството води листа на средства за создавање на квалификуван електронски потпис или печат, врз основа на податоците добиени од извештаите на лабораторијата. Лабораторијата без одлагање, а најдоцна во рок од 7 дена од денот на настаната промена е должна да го извести министерството за информатичко општество и администрација за издавање или одземање на потврда за сообразност на средствата за создавање на квалификувани електронски потписи и квалификувани електронски печати.

Министерот за информатичко општество и администрација ја пропишува содржината и начинот на водењето на листата од ставот 4 на овој член, начинот на поднесување на

барање регистрација во листата, потребните документи со барањето, како и начинот за барање за регистрација во листата.

Содржината на потврдата за сообразност на средство за создавање на квалификувани електронски потписи и квалификувани електронски печати и начинот на нејзино издавање ја пропишува министерот за информатичко општество и администрација со соодветен подзаконски акт.

Средствата кои се сертифицирани во акредитирани лаборатории во земја членка на Европската унија се признаваат и во Република Македонија.

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

Валидација на квалификуван електронски потпис и квалификуван електронски печат

Член 46

Процесот на валидација на квалификуван електронски потпис и 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 печатирањето претставува квалификуван електронски сертификат;
- 2) дали квалификуваниот сертификат бил издаден од давател на квалификувана доверлива услуга и бил валиден во времето на потпишување или печатирање;
- 3) дека податоците за валидација на потписот или печатот се соодветни со податоците дадени на засегнатата страна;
- 4) дека единствениот збир на податоци кои го претставуваат потписникот или управувачот со печатот во квалификуваниот сертификат, кои се дадени на засегнатата страна, се точни;
- 5) во случај на користење на псевдоним во времето на потпишување или печатирање, дали истото и е јасно укажано на засегнатата страна,
- 6) дали електронскиот потпис или печат бил создаден од средство за создавање на квалификуван електронски потпис или печат;
- 7) дека интегритетот на податоци кои се потпишани или печатирани не е компромитиран;
- 8) дека ги исполнуваат условите пропишани со член 38 и член 39 од овој закон во времето на потпишување или печатирање.

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

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

Член 47

Квалификувана услуга за валидација на квалификуван електронски потпис или печат може да биде обезбедена единствено од давател на квалификувани доверливи услуги и тоа:

- 1) постапката за валидација на квалификуван електронски потпис или печат е спроведена во согласност со член 46 на овој закон;
- 2) на засегнатата страна и овозможува да го добие резултатот од процесот на валидација на автоматизиран начин, кој е сигурен и ефикасен;

3) дека резултатот од процесот на проверка од точка 2) од овој став е печетиран со напреден електронски печат или потпишан со напреден електронски потпис од давателот на квалификувани доверливи услуги.

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

Стандардите кои треба да ги содржат потврдите за валидација на квалификуван електронски потпис или печат ги пропишува министерот за информатичко општество и администрација со правилник.

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

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

Член 48

Квалификувана доверлива услуга за чување на квалификувани електронски потписи или печати може да биде обезбедена единствено од давател на квалификувани доверливи услуги кој користи процедури и технологии осопособени да ја продолжат веродостојноста на квалификуваниот електронски потпис или печат и по истекот на период на важење обезбеден преку користење на технолошки средства.

Стандардите кои треба да ги исполни квалификуваната доверлива услуга за чување на квалификувани електронски потписи или печат ги пропишува министерот за информатичко општество и администрација со правилник.

Правно дејство на електронскиот потпис

Член 49

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

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

Правно дејство на електронскиот печат

Член 50

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

Квалификуваниот електронски печат е основа за презумпција за интегритетот на податоците и за точноста на потеклото на податоците врз основа на кои истиот е издаден.

6. Електронски временски жиг

Услови за кои треба да ги исполни квалификуваниот електронски временски жиг

Член 51

Квалификуваниот електронски временски жиг задолжително треба да 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) да се заснова на прецизен извор за време поврзан со утврден меѓународен стандард за време,
- 3) да е печатиран со напреден електронски печат или потпишан со напреден електронски потпис од давателот на квалификувани доверливи услуги.

Правно дејство на електронските временски жигови

Член 52

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

Квалификуваниот електронски временски жиг е основа за презумпција за точноста на датумот и времето кои се наведени, како и интегритетот на податоците на кои се однесуваат датумот и времето.

Квалификуваниот сертификат за електронски временски жиг издаден од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа. Стандардите кои треба да ги содржат квалификуваните сертификати за електронски временски жиг ги пропишува министерот за информатичко општество и администрација со правилник.

7. Електронска достава

Услови за вршење на квалификувана електронска препорачана достава

Член 53

Квалификуваната електронска препорачана достава задолжително треба да ги исполнува следните услови:

- 1) да е обезбедена преку еден или повеќе даватели на квалификувани доверливи услуги;
- 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 квалификувани доверливи услуги 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 наведено преку употреба на електронски временски жиг;
- 7) да обезбеди сигурност дека се исполнети условите поединечно за секој давател на услуги за електронска препорачана достава во случаите кога податоците се пренесуваат помеѓу два или повеќе даватели на услуги за електронска препорачана достава.

Правно дејство на квалификуваната електронска препорачана достава

Член 54

Не може да се оспорува доказната сила на податоците испратени или примени преку електронска препорачана достава само затоа што се во електронска форма или затоа што не ги исполнуваат условите за квалификувана електронска препорачана достава.

При размена на податоци преку квалификувана електронска препорачана достава се претпоставува интегритетот на податоците, испраќањето на податоците од утврдениот испраќач, нивниот прием од утврдениот примач, како и точноста на датумот и времето на испраќање и примање означени од давателот на услугата квалификувана електронска препорачана достава.

Потврдата за квалификувана електронска препорачана достава издадена од давател на квалификувана доверлива услуга има иста правна и доказна сила како јавна исправа. Стандардите кои треба да ги содржат потврдите за квалификувана електронска препорачана достава ги пропишува министерот за информатичко општество и администрација со правилник.

8. Проверка на автентичност на веб страници

Квалификуван сертификат за автентичност на веб страници

Член 55

Квалификуваниот сертификат за автентичност на веб страници треба да ги исполнува условите и стандардите определени во соодветен подзаконски акт донесен од страна на министерот за информатичко општество и администрација.

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.

9. Електронско складирање на документи

Подготовка на документи за електронско складирање

Член 57

Подготовката на документи за електронски 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.

Во документот подготвен за електронско складирање, може да бидат вклучени и метаподатоци.

Подготовка на документи за сигурносно електронско складирање и квалификувано електронско складирање

Член 58

Подготовката на документи за 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 за интегритетот и точноста 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.

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

Подготовката на документи за сигурносно квалификувано 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 и точноста на оригиналниот документ, како и за неговите прилози, се употребени квалификуван електронски потпис или 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.

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

Владата, на предлог на министерството за информатичко општество и администрација поблиску ги пропишува условите кои мора да бидат исполнети 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 електронско складирање на документи

Член 59

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 соодветни постапки и технолошки решенија.

Сигурносно електронско чување на документи кои се изготвени во согласност со членот 58 од овој закон, на кои е нанесен електронски потпис или печат и електронски временски жиг на начин определен во член 58 став 1 точка 4) со цел да се потврди интегритетот на оригиналниот документ и точноста, како и на неговите прилози, се

врши така што во текот на постапката за складирање се користат соодветни технолошки решенија.

Сигурносно квалификувано електронско складирање на документи кои во нивната оригинална форма содржат квалификуван 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 соодветни постапки и технолошки решенија.

Сигурносно електронско чување на документи кои се изготвени во согласност со членот 58 од овој закон, на кои е нанесен квалификуван електронски потпис или печат и квалификуван електронски временски жиг на начин определен во член 58 став 1 точка 4) со цел да се потврди интегритетот на оригиналниот документ и точноста, како и на неговите прилози.

Министерот за информатичко општество и администрација ги пропишува условите за спроведување на процедурите и технолошки решенија определени со овој член.

Услуги за електронско складирање и квалификувано електронско складирање на документи

Член 60

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, во согласност со одредбите од овој закон.

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

За документ кој се чува во рамките на услугите на електронско складирање на документи постои правна претпоставка за верност на оригиналниот документ, за кој давателот на услугата електронско складирање на документи издава соодветен сертификат.

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, тогаш оригиналниот документ може да биде уништен, освен ако не е поинаку определено со закон.

Услуги за квалификувано електронско складирање на документи ги обезбедува давател на квалификувани доверливи услуги, 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.

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 печат.

За документ кој се чува во рамките на услугите на квалификувани 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.

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.

Министерот за информатичко општество и администрација може со правилник да утврди стандарди кои треба да ги исполнуваат услугите за електронско складирање и квалификувано електронско складирање на документи.

VI. ЕЛЕКТРОНСКИ ОВЛАСТУВАЊА

Регистар на овластувања

Член 61

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

Овластувањето се издава со користење на електронски идентификација на властодателот и со потпишување на овластувањето со квалификуван електронски потпис.

Властодателот ги определува дејствијата за кои ги издава овластувањето, обемот и рокот на важноста на истото.

Регистарот на овластувања може да го водат само квалификувани даватели на доверливи услуги и издавачите на шеми за електронска идентификација.

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

Писмена форма

Член 62

Овластувањата евидентирани во регистарот на овластувања согласно член 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

Регистарот на овластувања нема карактер на јавна книга.

Властодателите, овластените лица и засегнатите страни имаат пристап до податоците од регистарот, кои се однесуваат на соодветното овластување поврзано со нив.

VII. НАДЗОР

Надзор над давателите на доверливи услуги и давателите на квалификувани доверливи услуги во електронски трансакции

Член 65

Надзор над примената на овој закон вршат овластени лица од министерството за информатичко општество и администрација, по претходно овластување од министерот за информатичко општество и администрација.

Овластените лица од ставот 1 на овој член вршат надзор над исполнетоста на условите утврдени со овој закон и прописите донесени за спроведување на овој закон.

Обем на овластување за вршење на надзор

Член 66

Овластените лица од членот 65 на овој закон може да:

- 1) наредат отстранување на неправилностите со определување на рок во кои неправилностите ќе бидат отстранети;
- 2) наредат да се забрани употреба на несоодветна инфраструктура и процедури со определување на рок во кој давателот на услугата е должен да обезбеди соодветни постапки и соодветна инфраструктура;
- 3) привремено да се забрани обезбедување на услугите, се до моментот на обезбедување на соодветни постапки и инфраструктура од страна на давателот на квалификувани доверливи услуги;
- 4) наредат привремено одземање на некои или на сите сертификати издадени од страна на давателот на услугата, доколку постои основано сомневање за несоодветно постапување или фалсификување.

VIII. ПРЕКРШОЧНИ ОДРЕДБИ

Член 67

Со парична казна од 5.000 до 10.000 евра во денарска противвредност ќе се казни давателот на квалификувани доверливи услуги - правно лице, ако:

- 1) не ги преземе потребните технички и организациски мерки за управување со ризиците кои ја загрозуваат сигурноста при обезбедување на доверливи услуги;
- 2) без одлагање, а најдоцна во рок од 24 часа од моментот на дознавање, не го извести министерството за информатичко општество и администрација 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;
- 3) 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;
- 4) пред склучувањето на договорот од членот 28 став 1 на овој закон не го извести лицето кое го поднело барањето за користење на квалификувани доверливи услуги за сите релевантни околности кои влијаат на услугата во согласност со член 28 став 2;
- 5) не ги исполнува условите од член 29;
- 6) при издавање на квалификувани сертификати за доверливи услуги не ги провери информациите за идентитетот на физичко или правно лице содржани во квалификуваниот сертификат, во согласност со член 31 став 2;
- 7) не ја провери усогласеноста со условите пред започнувањето на обезбедување квалификувани услуги на доверба или најмалку еднаш на секои 24 месеци;
- 8) пред да започне со вршење на дејноста давател на квалификувани доверливи услуги не е запишан во Регистарот на даватели на доверливи услуги и на шеми за електронска идентификација;
- 9) 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 за информатичко општество и администрација, најдоцна три месеци пред планираниот престанок на вршење на дејноста;
- 10) во случај на престанок на вршење на дејноста давател на квалификувани доверливи услуги не ги достави сите потребни технички средства во однос на обезбедување на

услуги до друг давател на квалификувани доверливи услуги на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги;

11) во случај на престанок на вршење на дејноста давател на квалификувани доверливи услуги не ја достави целокупната документација во однос на обезбедување на услуги до друг давател на квалификувани доверливи услуги на кој ја пренесува обврската за вршење на една или повеќе доверливи услуги или до министерството за информатичко општество и администрација;

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

13) издавачот на сертификати за квалификуван електронски потпис или печат не ги отповика издадените сертификати во случаите наведени во член 42 став 1;

14) издавачот 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;

15) на издавачот 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;

16) не обезбеди приклучување на Централниот систем за размена на достава преку квалификувана електронска испорака;

17) сигурносното електронско складирање и квалификувано електронско складирање на документи не е спроведено во согласност со член 58 од овој закон;

За прекршокот од ставот 1 на овој член ќе му се изрече парична казна од 1.000 до 5.000 евра во денарска противвредност одговорното лице на правното лице давател на квалификувани доверливи услуги.

Со парична казна од 5.000 до 10.000 евра во денарска противвредност ќе се казни давателот на неквалификувани доверливи услуги - правно лице ако не го извести министерството за информатичко општество и администрација за вршење на дејноста, согласно член 24 од овој закон.

За прекршокот од ставот 3 на овој член ќе му се изрече парична казна од 1.000 до 5.000 евра во денарска противвредност одговорното лице на правното лице давател на неквалификувани доверливи услуги.

Член 68

Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни правно лице корисник на квалификувани доверливи услуги, во случај на промена на податоците наведени во член 31 став 3 на овој закон не го извести веднаш давателот на квалификувани доверливи услуги.

Со парична казна од 500 до 1.000 евра во денарска противвредност ќе се казни одговорното лице на правното лице корисник на квалификувани доверливи услуги, за прекршокот од ставот 1 на овој член.

Со парична казна од 100 до 300 евра во денарска противвредност ќе се казни физичкото лице корисник на квалификувани доверливи услуги, за прекршокот од ставот 1 на овој член.

Член 69

Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни правно лице давател на квалификувани доверливи услуги кој има регистрирана шема за електронска идентификација, ако:

1) шемата на електронска идентификација не ги исполнува условите од член 11 од овој закон и

2) 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 во согласност со член 18 од овој закон.

Со парична казна од 500 до 1.000 евра во денарска противвредност ќе се казни одговорното лице на правното лице давател на квалификувани доверливи услуги, за прекршокот од ставот 1 на овој член.

Член 70

Со парична казна од 7.000 до 15.000 евра во денарска противвредност ќе се казни правно лице давател на квалификувани доверливи услуги, ако не постапи по наредба на овластеното лице за надзор во рок определен согласно член 65 од овој закон.

Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни одговорното лице на правното лице давател на квалификувани доверливи услуги, за прекршокот од ставот 1 на овој член.

Член 71

Со парична казна од 7.000 до 15.000 евра во денарска противвредност ќе се казни јавен орган кој нема да ја признае важноста или ќе ја оспори доказна сила на електронскиот документ изготвен во согласност со овој закон или дигитализиран документ создаден во согласност со членот 10 од овој закон, само затоа што тоа е електронски документ.

Со парична казна од 1.000 до 5.000 евра во денарска противвредност ќе се казни 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 во согласност со овој закон, само затоа што се издадени или употребени во електронски формат.

IX. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 72

Подзаконските акти определени со овој закон ќе бидат донесени во рок од 3 месеци од денот на неговото влегување во сила.

Член 73

Електронските потписи издадени согласно Законот за податоците во електронски облик и електронски потпис („Службен весник на Република Македонија“ бр. 34/2001, 6/2002, 98/2008 и 33/2015) продолжуваат да важат се до истекот на нивната важност.

Член 74

Давателите на доверливи услуги 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 во рок од една година, сметано од денот на влегување во сила на овој закон.

Во периодот на усогласување со одредбите на овој закон, давателите на доверливи услуги од ставот 1 на овој член ги обезбедуваат услугите за издавање на сертификати за електронски потписи и временски жигови без да бидат регистрирани.

Член 75

Овој закон влегува во сила и ќе започне да се применува осмиот ден од денот на објавувањето во "Службен весник на Република Македонија".

Законот за податоците во електронски облик и електронски потпис престанува да важи со денот на примената на овој закон.

Со денот на влегувањето на Република Македонија во Европската Унија престанува да важи овој закон и ќе се применува Регулативата eIDAS.

DRAFT