NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 910/2014

z 23. júla 2014

o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([1]),

konajúc v súlade s riadnym legislatívnym postupom ([2]),

keďže:

(1) Budovanie dôvery v prostredí online je kľúčom k hospodárskemu a sociálnemu rozvoju. V dôsledku nedostatku dôvery spôsobeného najmä pociťovaným nedostatkom právnej istoty spotrebitelia, podniky a orgány verejnej správy váhajú s realizáciou elektronických transakcií a prijímaním nových služieb.

(2) Cieľom tohto nariadenia je posilniť dôveru pri elektronických transakciách na vnútornom trhu zabezpečením spoločného základu pre bezpečné elektronické interakcie medzi občanmi, podnikmi a orgánmi verejnej správy, čím sa zvýši účinnosť verejných a súkromných služieb online, elektronického podnikania a elektronického obchodu v Únii.

(3) Smernica Európskeho parlamentu a Rady 1999/93/ES ([3]) sa vzťahovala na elektronické podpisy bez toho, aby poskytla komplexný cezhraničný a medziodvetvový rámec pre bezpečné, dôveryhodné a ľahko použiteľné elektronické transakcie. Týmto nariadením sa posilňuje a rozširuje *acquis* uvedenej smernice.

(4) V oznámení Komisie z 26. augusta 2010 s názvom Digitálna agenda pre Európu sa ako najväčšie prekážky pozitívneho kolobehu digitálneho hospodárstva identifikovali fragmentácia digitálneho trhu, nedostatočná interoperabilita a nárast počítačovej kriminality. Komisia v správe o občianstve EÚ za rok 2010 s názvom Odstránenie prekážok vykonávania práv občanov Únie ďalej zdôraznila potrebu vyriešiť hlavné problémy, ktoré bránia občanom Únie vo využívaní výhod jednotného digitálneho trhu a cezhraničných digitálnych služieb.

(5) Európska rada vo svojich záveroch zo 4. februára 2011 a 23. októbra 2011 vyzvala Komisiu, aby do roku 2015 vytvorila jednotný digitálny trh s cieľom dosiahnuť rýchly pokrok v kľúčových oblastiach digitálneho hospodárstva a podporiť v plnej miere integrovaný jednotný digitálny trh uľahčením cezhraničného používania služieb online a venovala pritom osobitnú pozornosť uľahčeniu bezpečnej elektronickej identifikácii a autentifikácii.

([1]) Ú. v. EÚ C 351, 15.11.2012, s. 73.
([2]) Pozícia Európskeho parlamentu z 3. apríla 2014 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 23. júla 2014.
([3]) Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy (Ú. v. ES L 13, 19.1.2000, s. 12).

(6) Rada vo svojich záveroch z 27. mája 2011 vyzvala Komisiu, aby prispela k jednotnému digitálnemu trhu vytvorením vhodných podmienok pre vzájomné uznávanie kľúčových cezhraničných prostriedkov, ako sú elektronická identifikácia, elektronické dokumenty, elektronické podpisy a elektronické doručovacie služby, a pre interoperabilné služby elektronickej verejnej správy v celej Európskej únii.

(7) Európsky parlament vo svojom uznesení z 21. septembra 2010 o dobudovaní vnútorného trhu v oblasti elektronického obchodu ([1]) zdôraznil význam bezpečnosti elektronických služieb, najmä elektronických podpisov, a potreby vytvoriť infraštruktúru verejných kľúčov na celoeurópskej úrovni, pričom vyzval Komisiu, aby vytvorila portál európskych orgánov overovania platnosti s cieľom zabezpečiť cezhraničnú interoperabilitu elektronických podpisov a zvýšiť bezpečnosť transakcií realizovaných prostredníctvom internetu.

(8) Smernica Európskeho parlamentu a Rady 2006/123/ES ([2]) vyžaduje, aby členské štáty vytvorili „miesta jednotného kontaktu“ s cieľom zabezpečiť, aby bolo možné ľahko splniť všetky postupy a formálne náležitosti vzťahujúce sa na prístup k činnostiam v oblasti služieb a na ich vykonávanie, a to na diaľku a elektronickými prostriedkami prostredníctvom príslušného miesta jednotného kontaktu a v súčinnosti s príslušnými orgánmi. Mnohé služby online prístupné prostredníctvom miest jednotného kontaktu si vyžadujú elektronickú identifikáciu, autentifikáciu a podpis.

(9) Vo väčšine prípadov občania nemôžu využívať svoju elektronickú identifikáciu na vlastnú autentifikáciu v inom členskom štáte, pretože vnútroštátne schémy elektronickej identifikácie v ich krajine nie sú uznané v iných členských štátoch. Táto elektronická bariéra bráni poskytovateľom služieb využívať výhody vnútorného trhu v plnej miere. Vzájomne uznávané prostriedky elektronickej identifikácie uľahčia cezhraničné poskytovanie početných služieb na vnútornom trhu a umožnia podnikom pôsobiť na cezhraničnom základe bez toho, aby čelili mnohým prekážkam pri interakcii s orgánmi verejnej správy.

(10) Smernicou Európskeho parlamentu a Rady 2011/24/EÚ ([3]) sa vytvára sieť vnútroštátnych orgánov zodpovedných za elektronické zdravotníctvo. S cieľom posilniť bezpečnosť a plynulosť cezhraničnej zdravotnej starostlivosti sa od tejto siete vyžaduje, aby vypracovala usmernenia pre cezhraničný prístup k elektronickým zdravotným údajom a službám, a to aj prostredníctvom podpory spoločných opatrení na identifikáciu a autentifikáciu s cieľom uľahčiť prenosnosť údajov v cezhraničnej zdravotnej starostlivosti. Vzájomné uznávanie elektronickej identifikácie a autentifikácie je kľúčom k realizácii cezhraničnej zdravotnej starostlivosti pre európskych občanov. Keď ľudia cestujú za ošetrením, ich zdravotné údaje musia byť prístupné v krajine ošetrenia. To si vyžaduje pevný, bezpečný a dôveryhodný rámec elektronickej identifikácie.

(11) Toto nariadenie by sa malo uplatňovať v úplnom súlade so zásadami týkajúcimi sa ochrany osobných údajov ustanovenými v smernici Európskeho parlamentu a Rady 95/46/ES ([4]). Z tohto hľadiska a so zreteľom na zásadu vzájomného uznávania ustanovenú v tomto nariadení by sa autentifikácia služby online mala týkať len spracúvania tých identifikačných údajov, ktoré sú primerané, relevantné a nie sú nadbytočné na účely poskytnutia prístupu k danej službe online. Okrem toho by poskytovatelia dôveryhodných služieb a orgány dohľadu mali rešpektovať požiadavky smernice 95/46/ES, ktoré sa týkajú dôvernosti a bezpečnosti spracovania údajov.

(12) Jedným z cieľov tohto nariadenia je odstrániť existujúce prekážky cezhraničného využívania prostriedkov elektronickej identifikácie, ktoré sa v členských štátoch používajú na autentifikáciu aspoň v prípade verejných služieb. Cieľom tohto nariadenia nie je zasahovať do oblasti systémov správy elektronickej identity a súvisiacich infraštruktúr vytvorených v členských štátoch. Cieľom tohto nariadenia je zabezpečiť, aby bola možná bezpečná elektronická identifikácia a autentifikácia pri prístupe k cezhraničným službám online, ktoré ponúkajú členské štáty.

([1]) Ú. v. EÚ C 50 E, 21.2.2012, s. 1.
([2]) Smernica Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu (Ú. v. EÚ L 376, 27.12.2006, s. 36).
([3]) Smernica Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti (Ú. v. EÚ L 88, 4.4.2011, s. 45).
([4]) Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31).

(13) Členské štáty by mali mať na účely elektronickej identifikácie naďalej možnosť používať alebo zaviesť prostriedky umožňujúce prístup k službám online. Mali by tiež mať možnosť rozhodovať o tom, či do poskytovania týchto prostriedkov zapoja súkromný sektor. Členské štáty by nemali byť povinné oznamovať svoje schémy elektronickej identifikácie Komisii. Členské štáty sa môžu rozhodnúť, či oznámia Komisii všetky, niektoré alebo neoznámia žiadne schémy elektronickej identifikácie používané na vnútroštátnej úrovni na prístup aspoň k verejným službám online alebo ku konkrétnym službám.

(14) V tomto nariadení je potrebné stanoviť určité podmienky, pokiaľ ide o to, ktoré prostriedky elektronickej identifikácie sa majú uznávať a ako by sa mali schémy elektronickej identifikácie oznamovať. Uvedené podmienky by členským štátom mali pomôcť pri budovaní potrebnej vzájomnej dôvery, pokiaľ ide o schémy elektronickej identifikácie, a pri vzájomnom uznávaní prostriedkov elektronickej identifikácie v rámci ich oznámených schém. Zásada vzájomného uznávania by sa mala uplatňovať vtedy, keď schéma elektronickej identifikácie oznamujúceho členského štátu spĺňa podmienky oznámenia a oznámenie bolo uverejnené v *Úradnom vestníku Európskej únie*. Zásada vzájomného uznávania by sa však mala týkať len autentifikácie služby online. Prístup k týmto službám online a ich konečné poskytnutie žiadateľovi by mali byť úzko spojené s právom na využívanie takýchto služieb na základe podmienok stanovených vo vnútroštátnych právnych predpisoch.

(15) Povinnosť uznať prostriedky elektronickej identifikácie by sa mala týkať len tých prostriedkov, ktorých úroveň zabezpečenia totožnosti zodpovedá rovnakej alebo vyššej úrovni, ako je úroveň požadovaná pre predmetnú službu online. Okrem toho by sa táto povinnosť mala uplatňovať len vtedy, keď dotknutý subjekt verejného sektora používa na prístup k danej službe online úrovne zabezpečenia „pokročilá“ alebo „vysoká“. Členským štátom by sa v súlade s právom Únie malo umožniť uznávať prostriedky elektronickej identifikácie s nižšími úrovňami zabezpečenia totožnosti.

(16) Úrovne zabezpečenia by mali charakterizovať stupeň dôveryhodnosti prostriedkov elektronickej identifikácie pri určovaní totožnosti osoby, čím by poskytovali záruku, že osoba hlásiaca sa k nejakej totožnosti, je naozaj osobou, ku ktorej bola daná totožnosť priradená. Úroveň zabezpečenia závisí od stupňa dôveryhodnosti, ktorý poskytuje daný prostriedok elektronickej identifikácie, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, pričom sa zohľadňujú používané procesy (napríklad preukazovanie totožnosti a overovanie a autentifikácia), riadiace činnosti (napríklad subjekt vydávajúci prostriedky elektronickej identifikácie a postup ich vydávania) a technické kontroly. Výsledkom rozsiahlych pilotných projektov financovaných prostriedkami Únie a normalizačných a medzinárodných činností sú rôzne technické vymedzenia a opisy úrovní zabezpečenia. Konkrétne, v rozsiahlom pilotnom projekte STORK a norme ISO 29115 sa okrem iného odkazuje na úrovne 2, 3 a 4, ktoré by sa mali pri vypracúvaní minimálnych technických požiadaviek, noriem a postupov pre úrovne zabezpečenia „nízka“, „pokročilá“ a „vysoká“ v zmysle tohto nariadenia v čo najväčšej miere zohľadňovať, pričom by sa malo zabezpečiť konzistentné uplatňovanie tohto nariadenia, najmä pokiaľ ide o úroveň zabezpečenia „vysoká“ týkajúcu sa preukazovania totožnosti na vydávanie kvalifikovaných certifikátov. Vypracované požiadavky by mali byť technologicky neutrálne. Dosiahnutie potrebných bezpečnostných požiadaviek by malo byť možné prostredníctvom rôznych technológií.

(17) Členské štáty by mali súkromný sektor nabádať, aby na účely identifikácie, ak je potrebná pri službách online alebo elektronických transakciách, dobrovoľne používal prostriedky elektronickej identifikácie z oznámenej schémy. Možnosť používať takéto prostriedky elektronickej identifikácie by súkromnému sektoru umožnila spoliehať sa na elektronickú identifikáciu a autentifikáciu, ktoré sa už vo veľkej miere používajú v mnohých členských štátoch prinajmenšom v rámci verejných služieb, a podnikom a občanom by uľahčila prístup k ich službám online naprieč hranicami. Na uľahčenie cezhraničného využívania takýchto prostriedkov elektronickej identifikácie súkromným sektorom by možnosť autentifikácie poskytovaná akýmkoľvek členským štátom mala byť dostupná pre spoliehajúce sa strany zo súkromného sektora, ktoré sú usadené mimo územia daného členského štátu, a to za rovnakých podmienok, aké platia pre spoliehajúce sa strany zo súkromného sektora, ktoré sú usadené v danom členskom štáte. Následne môže oznamujúci členský štát vymedziť v súvislosti so spoliehajúcimi sa stranami zo súkromného sektora podmienky prístupu k prostriedkom autentifikácie. Takéto podmienky prístupu môžu obsahovať informácie o tom, či sú prostriedky autentifikácie súvisiace s oznámenou schémou v súčasnosti dostupné pre spoliehajúce sa strany zo súkromného sektora.

(18) V tomto nariadení by sa mala ustanoviť zodpovednosť oznamujúceho členského štátu, strany vydávajúcej prostriedky elektronickej identifikácie a strany realizujúcej postup autentifikácie za nesplnenie príslušných povinností podľa tohto nariadenia. Toto nariadenie by sa však malo uplatňovať v súlade s vnútroštátnymi normami o zodpovednosti. Preto ním nie sú dotknuté uvedené vnútroštátne normy, napríklad o vymedzení pojmu škoda alebo príslušné uplatniteľné procesné normy vrátane dôkazného bremena.

(19) Bezpečnosť schém elektronickej identifikácie je kľúčom k dôveryhodnému cezhraničnému vzájomnému uznávaniu prostriedkov elektronickej identifikácie. V tomto kontexte by členské štáty mali na úrovni Únie spolupracovať v súvislosti s bezpečnosťou a interoperabilitou schém elektronickej identifikácie. Ak by si schémy elektronickej identifikácie vyžadovali, aby spoliehajúce sa strany na vnútroštátnej úrovni použili konkrétny hardvér alebo softvér, zo zásady cezhraničnej interoperability pre tieto členské štáty vyplýva, že nesmú takéto požiadavky a znášanie súvisiacich nákladov ukladať spoliehajúcim sa stranám usadeným mimo ich územia. V takomto prípade by sa v medziach rámca interoperability mali prerokovať a vypracovať primerané riešenia. Nemožno sa však vyhnúť technickým požiadavkám vyplývajúcim z inherentných špecifikácií vnútroštátnych prostriedkov elektronickej identifikácie, ktoré budú mať pravdepodobne vplyv na držiteľov takýchto elektronických prostriedkov (napr. čipových kariet).

(20) Spolupráca členských štátov by mala uľahčovať technickú interoperabilitu oznámených schém elektronickej identifikácie s cieľom podporiť vysokú mieru dôvery a bezpečnosti, primeranú stupňu rizika. Takejto spolupráci by mala pomáhať výmena informácií a najlepších postupov medzi členskými štátmi s cieľom zabezpečiť vzájomné uznávanie.

(21) Týmto nariadením by sa ďalej mal stanoviť všeobecný právny rámec pre používanie dôveryhodných služieb. Nemala by sa ním však stanoviť všeobecná povinnosť používať tieto služby, ani zriadiť prístupový bod pre všetky existujúce dôveryhodné služby. Predovšetkým by sa nemalo vzťahovať na poskytovanie služieb, ktoré sa používajú výhradne v uzatvorených systémoch medzi vymedzenými skupinami účastníkov a ktoré nemajú žiaden vplyv na tretie strany. Požiadavky tohto nariadenia by sa napríklad nemali týkať systémov, ktoré zriadili podniky alebo orgány verejnej správy na riadenie vnútorných postupov a v rámci ktorých sa využívajú dôveryhodné služby. Požiadavky tohto nariadenia by mali spĺňať len dôveryhodné služby poskytované verejnosti, ktoré majú vplyv na tretie strany. Toto nariadenie by sa nemalo vzťahovať ani na aspekty súvisiace s uzatváraním a platnosťou zmlúv alebo iných právnych záväzkov, pri ktorých existujú požiadavky na formu stanovené vo vnútroštátnom práve alebo práve Únie. Nemalo by mať ani vplyv na vnútroštátne požiadavky na formu v súvislosti s verejnými registrami, a to konkrétne obchodným registrom a katastrom nehnuteľností.

(22) S cieľom prispieť k všeobecnému cezhraničnému používaniu dôveryhodných služieb by malo byť možné používať ich ako dôkazy v súdnom konaní vo všetkých členských štátoch. Pokiaľ sa v tomto nariadení neustanovuje inak, vymedzenie právneho účinku dôveryhodných služieb sa ponecháva na vnútroštátne právo.

(23) Pokiaľ sa v tomto nariadení ustanovuje povinnosť uznávať dôveryhodnú službu, takúto dôveryhodnú službu je možné odmietnuť len vtedy, ak ju nie je adresát povinnosti schopný prečítať alebo overiť z technických dôvodov, na ktoré nemá adresát bezprostredný dosah. Táto povinnosť by však sama osebe nemala znamenať pre verejný subjekt požiadavku, aby zabezpečil potrebný hardvér a softvér na technickú čitateľnosť všetkých existujúcich dôveryhodných služieb.

(24) Členské štáty môžu v súlade s právom Únie zachovať alebo zaviesť vnútroštátne ustanovenia týkajúce sa dôveryhodných služieb, pokiaľ tieto služby nie sú plne harmonizované týmto nariadením. Na vnútornom trhu by však mal byť možný voľný obeh dôveryhodných služieb, ktoré sú v súlade s týmto nariadením.

(25) Členské štáty by mali mať možnosť voľne definovať ďalšie druhy dôveryhodných služieb popri tých, ktoré sú súčasťou uzavretého dôveryhodného zoznamu služieb ustanoveného v tomto nariadení, na účely ich uznania na vnútroštátnej úrovni ako kvalifikovaných dôveryhodných služieb.

(26) Vzhľadom na rýchlosť technologických zmien by sa v rámci tohto nariadenia mal prijať prístup, ktorý je otvorený inovácii.

(27) Toto nariadenie by malo byť technologicky neutrálne. Právne účinky, ktoré zaručuje, by malo byť možné dosiahnuť akýmikoľvek technickými prostriedkami za predpokladu, že sa splnia požiadavky uvedené v tomto nariadení.

(28) S cieľom posilniť najmä dôveru malých a stredných podnikov (ďalej len „MSP“) a spotrebiteľov vo vnútorný trh a podporiť používanie dôveryhodných služieb a produktov by sa mali zaviesť pojmy kvalifikované dôveryhodné služby a kvalifikovaný poskytovateľ dôveryhodných služieb na účel uvedenia požiadaviek a povinností, ktoré zabezpečia vysokú úroveň bezpečnosti akýchkoľvek používaných alebo poskytovaných kvalifikovaných dôveryhodných služieb a produktov.

(29) V súlade so záväzkami podľa Dohovoru Organizácie Spojených národov o právach osôb so zdravotným postihnutím, schváleného rozhodnutím Rady 2010/48/ES [1], a najmä článku 9 dohovoru, by osoby so zdravotným postihnutím mali mať možnosť využívať dôveryhodné služby a produkty pre koncových používateľov používané pri poskytovaní týchto služieb za rovnakých podmienok ako iní spotrebitelia. Poskytované dôveryhodné služby a produkty pre koncových používateľov používané pri poskytovaní týchto služieb by preto mali byť vždy, keď je to uskutočniteľné, prístupné osobám so zdravotným postihnutím. Posúdenie uskutočniteľnosti by malo okrem iného obsahovať technické a ekonomické zretele.

(30) Členské štáty by mali určiť orgán dohľadu alebo orgány dohľadu na vykonávanie činností dohľadu podľa tohto nariadenia. Členské štáty by mali tiež mať možnosť na základe vzájomnej dohody s iným členským štátom rozhodnúť o určení orgánu dohľadu na území tohto iného členského štátu.

(31) Orgány dohľadu by mali spolupracovať s orgánmi na ochranu osobných údajov, napríklad prostredníctvom ich informovania o výsledkoch auditov kvalifikovaných poskytovateľov dôveryhodných služieb v prípade podozrenia z porušenia predpisov o ochrane osobných údajov. Poskytovanie informácií by sa malo vzťahovať najmä na bezpečnostné incidenty a narušenia bezpečnosti osobných údajov.

(32) Povinnosťou všetkých poskytovateľov dôveryhodných služieb by malo byť uplatňovanie osvedčeného bezpečnostného postupu primeraného rizikám súvisiacim s ich činnosťami s cieľom posilniť dôveru používateľov v jednotný trh.

(33) Ustanovenia o používaní pseudonymov v certifikátoch by nemali členským štátom brániť v tom, aby vyžadovali identifikáciu osôb podľa práva Únie alebo vnútroštátneho práva.

(34) Všetky členské štáty by mali dodržiavať spoločné základné požiadavky v oblasti dohľadu s cieľom zabezpečiť porovnateľnú úroveň bezpečnosti kvalifikovaných dôveryhodných služieb. S cieľom uľahčiť konzistentné uplatňovanie týchto požiadaviek v celej Únii by členské štáty mali prijať porovnateľné postupy a mali by si vymieňať informácie o svojich činnostiach dohľadu a najlepších postupoch v tejto oblasti.

(35) Požiadavky tohto nariadenia, najmä požiadavky týkajúce sa bezpečnosti a povinnosti zaistiť náležitú starostlivosť, transparentnosť a zodpovednosť za svoje operácie a služby by sa mali vzťahovať na všetkých poskytovateľov dôveryhodných služieb. Vzhľadom na druh služieb, ktoré poskytujú poskytovatelia dôveryhodných služieb, je v súvislosti s týmito požiadavkami vhodné rozlišovať medzi kvalifikovanými a nekvalifikovanými poskytovateľmi dôveryhodných služieb.

(36) Vytvorením režimu dohľadu pre všetkých poskytovateľov dôveryhodných služieb by sa mali zabezpečiť rovnaké podmienky pre bezpečnosť a zodpovednosť ich operácií a služieb, čím by sa prispelo k ochrane používateľov a fungovaniu vnútorného trhu. Na nekvalifikovaných poskytovateľov dôveryhodných služieb by sa mali vzťahovať mierne a reaktívne následné činnosti dohľadu, odôvodnené povahou ich služieb a operácií. Orgán dohľadu by preto nemal mať žiadnu všeobecnú povinnosť dohliadať na nekvalifikovaných poskytovateľov služieb. Orgán dohľadu by preto mal konať len v prípade, ak získa informácie (napríklad od samotného nekvalifikovaného poskytovateľa dôveryhodných služieb, iného orgánu dohľadu, prostredníctvom oznámenia od používateľa alebo obchodného partnera, alebo na základe vlastného vyšetrovania), že nekvalifikovaný poskytovateľ dôveryhodných služieb nespĺňa požiadavky tohto nariadenia.

[1] Rozhodnutie Rady 2010/48/ES z 26. novembra 2009 o uzatvorení Dohovoru Organizácie Spojených národov o právach osôb so zdravotným postihnutím Európskym spoločenstvom (Ú. v. EÚ L 23, 27.1.2010, s. 35).

(37) V tomto nariadení by sa mala ustanoviť zodpovednosť všetkých poskytovateľov dôveryhodných služieb. Predovšetkým sa v ňom ustanovuje režim zodpovednosti, v rámci ktorého by mali všetci poskytovatelia dôveryhodných služieb zodpovedať za škody spôsobené akejkoľvek fyzickej alebo právnickej osobe z dôvodu nesplnenia si povinnosti podľa tohto nariadenia. Na uľahčenie posudzovania finančného rizika, ktoré by asi poskytovatelia dôveryhodných služieb museli znášať alebo ktoré by mali vykrývať poistením, im toto nariadenia umožňuje stanovovať za určitých podmienok obmedzenia týkajúce sa používania služieb, ktoré poskytujú, a nezodpovedať za škody, ktoré vyplynú z používania služieb presahujúcich takéto obmedzenia. Zákazníci by mali byť o takýchto obmedzeniach vopred riadne informovaní. Uvedené obmedzenia by mala byť schopná pochopiť aj tretia strana, napríklad prostredníctvom začlenenia informácií o týchto obmedzeniach do podmienok poskytovania danej služby alebo prostredníctvom iných pochopiteľných prostriedkov. Na účely nadobudnutia účinnosti týchto zásad by sa malo toto nariadenie uplatňovať v súlade s vnútroštátnymi normami o zodpovednosti. Preto týmto nariadením nie sú dotknuté uvedené vnútroštátne normy, napríklad o vymedzení pojmu škoda, úmysel, nedbanlivosť, alebo príslušné uplatniteľné procesné normy.

(38) Oznamovanie narušení bezpečnosti a posúdení bezpečnostných rizík je zásadné pre poskytnutie primeraných informácií zúčastneným stranám v prípade narušenia bezpečnosti alebo integrity.

(39) Aby Komisia a členské štáty mohli posúdiť efektívnosť mechanizmu oznamovania narušenia zavedeného týmto nariadením, malo by sa vyžadovať, aby orgány dohľadu poskytovali Komisii a Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) súhrnné informácie.

(40) Aby Komisia a členské štáty mohli posúdiť efektívnosť rozšíreného mechanizmu dohľadu zavedeného týmto nariadením, malo by sa vyžadovať, aby orgány dohľadu podávali správy o svojich činnostiach. Bolo by to dôležité pre uľahčenie výmeny osvedčených postupov medzi orgánmi dohľadu a zabezpečilo by sa tým overenie konzistentného a účinného vykonávania základných požiadaviek dohľadu vo všetkých členských štátoch.

(41) S cieľom zabezpečiť trvalú udržateľnosť a trvácnosť kvalifikovaných dôveryhodných služieb a posilniť dôveru používateľov v kontinuitu kvalifikovaných dôveryhodných služieb by orgány dohľadu mali overovať existenciu a správne uplatňovanie ustanovení o plánoch ukončenia činnosti v prípade, že kvalifikovaní poskytovatelia dôveryhodných služieb prestanú vykonávať svoju činnosť.

(42) S cieľom uľahčiť dohľad nad kvalifikovanými poskytovateľmi dôveryhodných služieb, napríklad keď poskytovateľ poskytuje svoje služby na území iného členského štátu, kde nepodlieha dohľadu, alebo keď sa počítače poskytovateľa nachádzajú na území iného členského štátu ako toho, v ktorom je usadený, by sa mal vytvoriť systém vzájomnej pomoci medzi orgánmi dohľadu v členských štátoch.

(43) S cieľom zabezpečiť, aby kvalifikovaní poskytovatelia dôveryhodných služieb a služby, ktoré poskytujú, spĺňali požiadavky stanovené v tomto nariadení, by mal orgán posudzovania zhody vykonávať posúdenia zhody a následne by kvalifikovaní poskytovatelia dôveryhodných služieb mali orgánu dohľadu zasielať správy o takomto posúdení. Vždy keď orgán dohľadu požiada kvalifikovaného poskytovateľa dôveryhodnej služby o poskytnutie ad hoc správy o posúdení zhody, mal by orgán dohľadu rešpektovať najmä zásady dobrej správy vecí verejných vrátane povinnosti odôvodniť svoje rozhodnutia, ako aj zásadu primeranosti. Preto by orgán dohľadu mal náležite odôvodniť svoje rozhodnutie, ktorým požaduje predloženie ad hoc správy o posúdení zhody.

(44) Cieľom tohto nariadenia je zabezpečiť koherentný rámec so zámerom poskytnúť vysokú úroveň bezpečnosti a právnej istoty pri dôveryhodných službách. Z tohto hľadiska by sa Komisia pri riešení posudzovania zhody produktov a služieb mala v relevantných prípadoch usilovať o synergie s existujúcimi príslušnými európskymi a medzinárodnými schémami, ako napríklad nariadením Európskeho parlamentu a Rady (ES) č. 765/2008 ([1]), ktorým sa stanovujú požiadavky akreditácie orgánov posudzovania zhody a dohľadu nad trhom s výrobkami.

([1]) Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

(45) S cieľom umožniť účinný iniciačný proces, ktorý by mal viesť k začleneniu kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú, do dôveryhodných zoznamov, by sa mali podporiť predbežné interakcie medzi potenciálnymi kvalifikovanými poskytovateľmi dôveryhodných služieb a príslušným orgánom dohľadu, aby sa uľahčila náležitá starostlivosť vedúca k poskytovaniu kvalifikovaných dôveryhodných služieb.

(46) Dôveryhodné zoznamy sú podstatnými prvkami pre vybudovanie dôvery medzi trhovými subjektmi, pretože určujú kvalifikovaný štatút poskytovateľa služieb v čase dohľadu.

(47) Aby mohli používatelia naplno využívať elektronické služby a uvedomovali si, že sa na ne môžu spoľahnúť, je nevyhnutné, aby služby online boli dôveryhodné a ich používanie pohodlné. Na tento účel by sa mala zaviesť značka dôvery EÚ, ktorou sa budú označovať kvalifikované dôveryhodné služby poskytované kvalifikovanými poskytovateľmi dôveryhodných služieb. Takouto značkou dôvery EÚ pre kvalifikované dôveryhodné služby by sa jasne rozlišovalo medzi kvalifikovanými dôveryhodnými službami a ostatnými dôveryhodnými službami, čím by sa prispelo k transparentnosti na trhu. Používanie značky dôvery EÚ zo strany kvalifikovaných poskytovateľov dôveryhodných služieb by malo byť dobrovoľné a nemalo by viesť k žiadnym dodatočným požiadavkám okrem tých, ktoré sú stanovené v tomto nariadení.

(48) Hoci na zabezpečenie vzájomného uznávania elektronických podpisov v osobitných prípadoch, ako napríklad v kontexte rozhodnutia Komisie 2009/767/ES ([1]), je potrebná vysoká úroveň bezpečnosti, mali by sa akceptovať aj elektronické podpisy s nižšou zárukou bezpečnosti.

(49) Týmto nariadením by sa mala ustanoviť zásada, že elektronickému podpisu by sa nemal odopierať právny účinok z dôvodu, že je v elektronickej forme alebo že nespĺňa požiadavky na kvalifikovaný elektronický podpis. Ponecháva sa však na vnútroštátne právo, aby vymedzilo právny účinok elektronických podpisov s výnimkou požiadavky stanovenej v tomto nariadení, podľa ktorej má kvalifikovaný elektronický podpis rovnocenný právny účinok ako vlastnoručný podpis.

(50) Keďže príslušné orgány v členských štátoch v súčasnosti používajú rozdielne formáty zdokonalených elektronických podpisov na elektronické podpisovanie svojich dokumentov, je nevyhnutné zabezpečiť, aby členské štáty po prijatí elektronicky podpísaných dokumentov mohli technicky podporovať aspoň niekoľko formátov zdokonalených elektronických podpisov. Podobne, keď príslušné orgány v členských štátoch používajú zdokonalené elektronické pečate, bolo by potrebné zabezpečiť, aby podporovali aspoň niektoré formáty zdokonalených elektronických pečatí.

(51) Podpisovateľ by mal mať možnosť zveriť kvalifikované zariadenia na vyhotovenie elektronického podpisu do starostlivosti tretej strany za predpokladu, že sa zavedú vhodné mechanizmy a postupy, ktorými sa zabezpečí, že podpisovateľ bude mať výlučnú kontrolu nad používaním svojich údajov na vyhotovenie elektronického podpisu a že pri používaní zariadenia budú splnené požiadavky na kvalifikovaný elektronický podpis.

(52) Vyhotovovanie elektronických podpisov na diaľku, keď rámec vyhotovovania elektronických podpisov riadi poskytovateľa dôveryhodných služieb v mene podpisovateľa, bude narastať vzhľadom na mnohé ekonomické výhody, ktoré prináša. Aby sa však zabezpečilo, že takéto elektronické podpisy budú z právneho hľadiska uznávané rovnako ako elektronické podpisy, ktoré sa vyhotovujú v rámci riadenom výlučne používateľom, poskytovatelia služby elektronického podpisu na diaľku by mali uplatňovať osobitné bezpečnostné postupy riadenia a správy a využívať dôveryhodné systémy a produkty zahŕňajúce zabezpečené kanály pre elektronickú komunikáciu, aby sa zabezpečila dôveryhodnosť rámca, v ktorom sa elektronické podpisy vyhotovujú, a aby sa zaručilo, že tento rámec sa používa pod výlučnou kontrolou podpisovateľa. Ak sa kvalifikovaný elektronický podpis vyhotovil pomocou zariadenia na vyhotovenie elektronického podpisu na diaľku, mali by sa uplatňovať požiadavky stanovené v tomto nariadení, ktoré sa vzťahujú na kvalifikovaných poskytovateľov dôveryhodných služieb.

([1]) Rozhodnutie Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu (Ú. v. EÚ L 274, 20.10.2009, s. 36).

(53) Pozastavovanie kvalifikovaných certifikátov je tradičnou prevádzkovou praxou poskytovateľov dôveryhodných služieb vo viacerých členských štátoch a odlišuje sa od zrušenia a vyznačuje sa dočasnou stratou platnosti certifikátu. V záujme právnej istoty je nevyhnutné, aby bol štatút pozastavenia certifikátu vždy jasne uvedený. Poskytovatelia dôveryhodných služieb by preto mali niesť zodpovednosť za jasné uvedenie štatútu certifikátu, a ak je tento pozastavený, presného obdobia, počas ktorého je certifikát pozastavený. Týmto nariadením by sa nemalo poskytovateľom dôveryhodných služieb alebo členským štátom ukladať, aby pozastavovanie využívali, ale mali by sa ním ustanoviť pravidlá transparentnosti v prípadoch, keď sa takýto postup využíva.

(54) Cezhraničná interoperabilita a uznávanie kvalifikovaných certifikátov je predpokladom pre cezhraničné uznávanie kvalifikovaných elektronických podpisov. Kvalifikované certifikáty by preto nemali podliehať žiadnym povinným požiadavkám prekračujúcim požiadavky stanovené v tomto nariadení. Na vnútroštátnej úrovni by sa však malo povoliť začlenenie konkrétnych atribútov, akými sú napríklad jedinečné identifikátory, do kvalifikovaných certifikátov, a to za predpokladu, že tieto konkrétne atribúty nebudú prekážkou pre cezhraničnú interoperabilitu ani uznávanie kvalifikovaných certifikátov a elektronických podpisov.

(55) Dôležitým nástrojom overovania bezpečnosti kvalifikovaných zariadení na vyhotovenie elektronických podpisov je bezpečnostná certifikácia IT založená na medzinárodných normách, ako napríklad norma ISO 15408 a súvisiace metódy hodnotenia a pravidlá v oblasti vzájomného uznávania, a mala by sa podporovať. Inovatívne riešenia a služby, ako napríklad podpisovanie cez mobilné zariadenia a cloud, však spočívajú na technických a organizačných riešeniach pre kvalifikované zariadenia na vyhotovenie elektronických podpisov, pre ktoré ešte nemusia byť bezpečnostné normy k dispozícii alebo pri ktorých prebieha prvá bezpečnostná certifikácia IT. Úroveň bezpečnosti takýchto kvalifikovaných zariadení na vyhotovenie elektronických podpisov by sa mohla hodnotiť prostredníctvom používania alternatívnych procesov len vtedy, ak takéto bezpečnostné normy nie sú k dispozícii, alebo ak prebieha prvá bezpečnostná certifikácia IT. Uvedené procesy by mali byť v prípade ich rovnocenných úrovní bezpečnosti porovnateľné s normami bezpečnostnej certifikácie IT. Uvedené procesy by sa mohli uľahčiť prostredníctvom partnerského preskúmania.

(56) Toto nariadenie by malo stanoviť požiadavky na kvalifikované zariadenie na vyhotovenie elektronických podpisov s cieľom zabezpečiť funkčnosť zdokonalených elektronických podpisov. Toto nariadenie by sa nemalo vzťahovať na celé systémové prostredie, v ktorom uvedené zariadenia pracujú. Preto by sa mal rozsah certifikácie kvalifikovaných zariadení na vyhotovenie podpisov obmedziť na hardvér a systémový softvér používaný na správu a ochranu údajov na vyhotovenie podpisu, ktoré sa tvoria, uchovávajú alebo spracúvajú v zariadení na vyhotovenie podpisov. Ako sa podrobne opisuje v príslušných normách, z rozsahu certifikačnej povinnosti by sa mali vylúčiť aplikácie na vyhotovenie podpisov.

(57) Na zabezpečenie právnej istoty v súvislosti s platnosťou podpisu je nevyhnutné určiť zložky kvalifikovaného elektronického podpisu, ktoré by mala posúdiť spoliehajúca sa strana vykonávajúca validáciu. Navyše určenie požiadaviek na kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí môžu poskytovať kvalifikovanú službu validácie spoliehajúcim sa stranám, ktoré nechcú alebo nemôžu samy vykonávať validáciu kvalifikovaných elektronických podpisov, by malo stimulovať súkromný a verejný sektor, aby investoval do takýchto služieb. Oba prvky by mali všetkým stranám na úrovni Únie uľahčiť a zjednodušiť validáciu kvalifikovaných elektronických podpisov.

(58) Keď sa pri transakcii vyžaduje kvalifikovaná elektronická pečať právnickej osoby, rovnako akceptovateľný by mal byť aj kvalifikovaný elektronický podpis splnomocneného zástupcu právnickej osoby.

(59) Elektronické pečate by mali slúžiť ako dôkaz, že elektronický dokument vydala právnická osoba, a zabezpečujú istotu, pokiaľ ide o pôvod a integritu dokumentu.

(60) Poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty pre elektronické pečate, by mali zaviesť potrebné opatrenia na to, aby mohli určiť totožnosť fyzickej osoby zastupujúcej právnickú osobu, ktorej sa poskytol kvalifikovaný certifikát pre elektronickú pečať, a to v prípade, ak je takáto identifikácia potrebná na vnútroštátnej úrovni v kontexte súdneho alebo správneho konania.

(61) Týmto nariadením by sa malo zaručiť dlhodobé uchovávanie informácií, aby sa zabezpečila právna platnosť elektronických podpisov a elektronických pečatí počas dlhších období, a aby sa zaručilo, že sa môžu validovať bez ohľadu na budúce technologické zmeny.

(62) Na zaistenie bezpečnosti kvalifikovaných elektronických časových pečiatok by sa týmto nariadením malo vyžadovať používanie zdokonalenej elektronickej pečate alebo zdokonaleného elektronického podpisu, alebo iných rovnocenných metód. Predpokladá sa, že inovácia môže viesť k novým technológiám, ktoré môžu zaistiť rovnocennú úroveň bezpečnosti časových pečiatok. Ak sa použije iná metóda ako zdokonalená elektronická pečať alebo zdokonalený elektronický podpis, kvalifikovaný poskytovateľ dôveryhodných služieb by mal v súlade s posúdením zhody preukázať, že táto metóda zaručuje rovnocennú úroveň bezpečnosti a je v súlade s povinnosťami stanovenými v tomto nariadení.

(63) Elektronické dokumenty sú dôležité pre ďalší rozvoj cezhraničných elektronických transakcií na vnútornom trhu. Týmto nariadením by sa mala ustanoviť zásada, že elektronickému dokumentu by sa nemal odopierať právny účinok z dôvodu, že je v elektronickej forme, aby sa zabezpečilo, že elektronický transakcia nebude odmietnutá len z dôvodu, že dokument je v elektronickej forme.

(64) Pri riešení formátu zdokonalených elektronických podpisov a pečatí by Komisia mala vychádzať z existujúcich postupov, noriem a právnych predpisov, a to najmä z rozhodnutia Komisie 2011/130/EÚ ([1]).

(65) Popri autentifikácii dokumentu vydaného právnickou osobou sa elektronické pečate môžu používať aj na autentifikáciu akéhokoľvek digitálneho majetku právnickej osoby, napríklad softvérového kódu alebo serverov.

(66) Je dôležité, aby sa ustanovil právny rámec na uľahčenie cezhraničného uznávania elektronických doručovacích služieb pre registrované zásielky medzi jednotlivými vnútroštátnymi právnymi systémami. Uvedený rámec by tiež mohol otvoriť nové trhové príležitosti pre poskytovateľov dôveryhodných služieb z Únie, aby mohli poskytovať nové celoeurópske elektronické doručovacie služby pre registrované zásielky.

(67) Služby autentifikácie webových sídiel umožňujú návštevníkom, aby sa uistili, že za daným webovým sídlom stojí skutočný a legitímny subjekt. Uvedené služby prispievajú k budovaniu dôvery a istoty v súvislosti s podnikaním online, keďže používatelia budú dôverovať autentifikovanému webovému sídlu. Poskytovanie a využívanie služieb autentifikácie webových sídiel je úplne dobrovoľné. Aby sa však autentifikácia webových sídiel stala prostriedkom na zvyšovanie dôvery, poskytovanie lepšej skúsenosti pre používateľa a podporu rastu na vnútornom trhu, mali by sa v tomto nariadení ustanoviť minimálne povinnosti týkajúce sa bezpečnosti a zodpovednosti poskytovateľov a ich služieb. Na tento účel sa zohľadnili výsledky existujúcich iniciatív vedených príslušným odvetvím, napríklad Certification Authorities/Browsers Forum – CA/B Forum. Okrem toho by toto nariadenie nemalo byť prekážkou pri využívaní iných prostriedkov alebo metód autentifikácie webových sídiel, ktoré nepatria do jeho rozsahu pôsobnosti, ani by sa ním nemalo brániť poskytovateľom služieb autentifikácie webových sídiel z tretích krajín, aby svoje služby poskytovali zákazníkom z Únie. Poskytovateľovi z tretej krajiny by sa však jeho služby autentifikácie webových sídiel mohli podľa tohto nariadenia uznať za kvalifikované len v prípade, ak sa uzavrela medzinárodná dohoda medzi Úniou a krajinou, v ktorej je tento poskytovateľ usadený.

(68) Pojem „právnické osoby“ podľa ustanovení Zmluvy o fungovaní Európskej únie (ZFEÚ) týkajúcich sa usadenia ponecháva subjektom voľnosť zvoliť si právnu formu, ktorú považujú za vhodnú na výkon svojej činnosti. „Právnické osoby“ sú teda v zmysle ZFEÚ všetky subjekty, ktoré boli zriadené podľa práva členského štátu alebo sa ním spravujú, a to bez ohľadu na ich právnu formu.

(69) Inštitúcie, orgány, úrady a agentúry Únie sa nabádajú, aby uznávali elektronickú identifikáciu a dôveryhodné služby, na ktoré sa vzťahuje toto nariadenie, na účely administratívnej spolupráce a využívali najmä existujúce osvedčené postupy a výsledky prebiehajúcich projektov v oblastiach, na ktoré sa vzťahuje toto nariadenie.

([1]) Rozhodnutie Komisie 2011/130/EÚ z 25. februára 2011, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu (Ú. v. EÚ L 53, 26.2.2011, s. 66).

(70) S cieľom doplniť určité podrobné technické aspekty tohto nariadenia pružným a rýchlym spôsobom by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ, pokiaľ ide o kritériá, ktoré majú splniť subjekty zodpovedné za certifikáciu kvalifikovaných zariadení na vyhotovenie elektronických podpisov. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov. Pri príprave a vypracúvaní delegovaných aktov by Komisia mala zabezpečiť, aby sa dokumenty súčasne, vo vhodnom čase a vhodným spôsobom postúpili Európskemu parlamentu a Rade.

(71) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci, najmä pokiaľ ide o špecifikovanie referenčných čísel noriem, ktorých použitie by zakladalo domnienku súladu s určitými požiadavkami stanovenými v tomto nariadení. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011 ([1]).

(72) Pri prijímaní delegovaných alebo vykonávacích aktov by Komisia mala náležite zohľadňovať normy a technické špecifikácie vypracované európskymi a medzinárodnými normalizačnými organizáciami a subjektmi, a to najmä Európskym výborom pre normalizáciu (CEN), Európskym inštitútom pre telekomunikačné normy (ETSI), Medzinárodnou organizáciou pre normalizáciu (ISO) a Medzinárodnou telekomunikačnou úniou (ITU), aby sa zaistila vysoká úroveň bezpečnosti a interoperability pri elektronickej identifikácii a dôveryhodných službách.

(73) Z dôvodu právnej istoty a jasnosti by sa mala zrušiť smernica 1999/93/ES.

(74) S cieľom zabezpečiť právnu istotu pre trhové subjekty, ktoré už používajú kvalifikované certifikáty vydané fyzickým osobám v súlade so smernicou 1999/93/ES, je nevyhnutné stanoviť dostatočné prechodné obdobie. Obdobne by sa mali ustanoviť prechodné opatrenia pre bezpečné zariadenia na vyhotovenie podpisu, ktorých zhoda bola potvrdená v súlade so smernicou 1999/93/ES, ako aj pre poskytovateľov certifikačných služieb, ktorí vydávajú kvalifikované certifikáty pred 1. júlom 2016. Napokon je tiež nevyhnutné, aby sa Komisii umožnilo prijať vykonávacie akty a delegované akty pred uvedeným dátumom.

(75) Dátumy začiatku uplatňovania stanovené v tomto nariadení nemajú vplyv na existujúce povinnosti, ktoré už členské štáty majú podľa práva Únie, najmä podľa smernice 2006/123/ES.

(76) Keďže ciele tohto nariadenia nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov, ale z dôvodu rozsahu činnosti ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie týchto cieľov.

(77) Európsky dozorný úradník pre ochranu údajov bol konzultovaný v súlade s článkom 28 ods. 2 nariadenia Európskeho parlamentu a Rady (ES) č. 45/2001 ([2]) a vydal stanovisko 27. septembra 2012 ([3]),

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

([2]) Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).

([3]) Ú. v. EÚ C 28, 30.1.2013, s. 6.

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

S cieľom zabezpečiť riadne fungovanie vnútorného trhu a so zameraním na primeranú úroveň bezpečnosti prostriedkov elektronickej identifikácie a dôveryhodných služieb sa týmto nariadením:

a) stanovujú podmienky, za ktorých členské štáty uznávajú prostriedky elektronickej identifikácie fyzických a právnických osôb, ktoré patria do oznámenej schémy elektronickej identifikácie iného členského štátu;

b) stanovujú pravidlá pre dôveryhodné služby, najmä elektronické transakcie, a

c) vytvára právny rámec pre elektronické podpisy, elektronické pečate, elektronické časové pečiatky, elektronické dokumenty, elektronické doručovacie služby pre registrované zásielky a certifikačné služby pre autentifikáciu webových sídiel.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa vzťahuje na schémy elektronickej identifikácie, ktoré boli oznámené členskými štátmi a na poskytovateľov dôveryhodných služieb, ktorí sú usadení v Únii.

2. Toto nariadenie sa nevzťahuje na poskytovanie dôveryhodných služieb, ktoré sa používajú výhradne v uzavretých systémoch na základe vnútroštátneho práva alebo dohôd medzi vymedzenou skupinou účastníkov.

3. Toto nariadenie nemá vplyv na vnútroštátne právo ani právo Únie súvisiace s uzatváraním a platnosťou zmlúv alebo iných právnych či procesných záväzkov týkajúcich sa formy.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňujú tieto vymedzenia pojmov:

1. „elektronická identifikácia“ je proces používania osobných identifikačných údajov v elektronickej forme, ktoré jedinečne reprezentujú fyzickú osobu alebo právnickú osobu alebo fyzickú osobu zastupujúcu právnickú osobu;

2. „prostriedok elektronickej identifikácie“ je hmotná jednotka a/alebo nehmotná jednotka obsahujúca osobné identifikačné údaje, ktorá sa používa na autentifikáciu pre služby online;

3. „osobné identifikačné údaje“ sú súbor údajov, ktorý umožňuje určiť totožnosť fyzickej osoby alebo právnickej osoby alebo fyzickej osoby zastupujúcej právnickú osobu;

4. „schéma elektronickej identifikácie“ je systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým osobám alebo právnickým osobám alebo fyzickým osobám zastupujúcim právnické osoby vydávajú prostriedky elektronickej identifikácie;

5. „autentifikácia“ je elektronický proces, ktorý umožňuje potvrdiť elektronickú identifikáciu fyzickej osoby alebo právnickej osoby alebo pôvod a integritu údajov v elektronickej forme;

6. „spoliehajúca sa strana“ je fyzická osoba alebo právnická osoba, ktorá sa spolieha na elektronickú identifikáciu alebo dôveryhodnú službu;

7. „subjekt verejného sektora“ je ústredný, regionálny alebo miestny orgán, verejnoprávny subjekt alebo združenie tvorené jedným alebo viacerými takýmito orgánmi alebo jedným či viacerými takýmito verejnoprávnymi subjektmi, alebo súkromný subjekt, ktorý aspoň jeden z takýchto orgánov, subjektov alebo združení poveril poskytovaním verejných služieb, keď koná na základe takéhoto poverenia;

8. „verejnoprávny subjekt“ je subjekt v zmysle článku 2 ods. 1 bodu 4 smernice Európskeho parlamentu a Rady 2014/24/EÚ ([1]);

9. „podpisovateľ“ je fyzická osoba, ktorá vyhotovuje elektronický podpis;

10. „elektronický podpis“ sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;

11. „zdokonalený elektronický podpis“ je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26;

12. „kvalifikovaný elektronický podpis“ je zdokonalený elektronický podpis vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy;

13. „údaje na vyhotovenie elektronického podpisu“ sú jedinečné údaje, ktoré podpisovateľ používa na vyhotovenie elektronického podpisu;

14. „certifikát pre elektronický podpis“ je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym;

15. „kvalifikovaný certifikát pre elektronický podpis“ je certifikát pre elektronický podpis, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe I;

16. „dôveryhodná služba“ je elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva:

    a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

    b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo

    c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia;

17. „kvalifikovaná dôveryhodná služba“ je dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky stanovené v tomto nariadení;

([1]) Smernica Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES (Ú. v. EÚ L 94, 28.3.2014, s. 65).

18. „orgán posudzovania zhody“ je orgán vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008, ktorý je v súlade s uvedeným nariadením akreditovaný ako orgán príslušný na posudzovanie zhody kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú;

19. „poskytovateľ dôveryhodných služieb“ je fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb;

20. „kvalifikovaný poskytovateľ dôveryhodných služieb“ je poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb a ktorému orgán dohľadu udelil kvalifikovaný štatút;

21. „produkt“ je hardvér alebo softvér alebo príslušné zložky hardvéru alebo softvéru určené na používanie pri poskytovaní dôveryhodných služieb;

22. „zariadenie na vyhotovenie elektronického podpisu“ je nakonfigurovaný softvér alebo hardvér používaný na vyhotovenie elektronického podpisu;

23. „kvalifikované zariadenie na vyhotovenie elektronického podpisu“ je zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II;

24. „pôvodca pečate“ je právnická osoba, ktorá vyhotovuje elektronickú pečať;

25. „elektronická pečať“ sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov;

26. „zdokonalená elektronická pečať“ je elektronická pečať, ktorá spĺňa požiadavky stanovené v článku 36;

27. „kvalifikovaná elektronická pečať“ je zdokonalená elektronická pečať vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať;

28. „údaje pre vyhotovenie elektronickej pečate“ sú jedinečné údaje, ktoré používa pôvodca elektronickej pečate na vyhotovenie elektronickej pečate;

29. „certifikát pre elektronickú pečať“ je elektronické osvedčenie, ktoré spája údaje na validáciu elektronickej pečate s právnickou osobou a potvrdzuje jej názov;

30. „kvalifikovaný certifikát pre elektronickú pečať“ je certifikát pre elektronickú pečať, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe III;

31. „zariadenie na vyhotovenie elektronickej pečate“ je nakonfigurovaný softvér alebo hardvér používaný na vyhotovenie elektronickej pečate;

32. „kvalifikované zariadenie na vyhotovenie elektronickej pečate“ je zariadenie na vyhotovenie elektronickej pečate, ktoré primerane spĺňa požiadavky stanovené v prílohe II;

33. „elektronická časová pečiatka“ sú údaje v elektronickej forme, ktoré viažu iné údaje v elektronickej forme s konkrétnym časom, čím tvoria dôkaz o existencii týchto iných údajov v danom čase;

34. „kvalifikovaná elektronická časová pečiatka“ je elektronická časová pečiatka, ktorá spĺňa požiadavky stanovené v článku 42;

35. „elektronický dokument“ je akýkoľvek obsah uložený v elektronickej forme, najmä text alebo zvukový, obrazový či audiovizuálny záznam;

36. „elektronická doručovacia služba pre registrované zásielky“ je služba, ktorá umožňuje posielanie údajov elektronickými prostriedkami medzi tretími stranami a poskytuje dôkaz týkajúci sa nakladania s odoslanými údajmi vrátane potvrdenia o odoslaní a doručení údajov a ktorá chráni odosielané údaje pred rizikom straty, krádeže, poškodenia alebo akýchkoľvek neoprávnených úprav;

37. „kvalifikovaná elektronická doručovacia služba pre registrované zásielky“ je elektronická doručovacia služba pre registrované zásielky, ktorá spĺňa požiadavky stanovené v článku 44;

38. „certifikát pre autentifikáciu webového sídla“ je osvedčenie, ktoré umožňuje autentifikáciu webového sídla a spája toto webové sídlo s fyzickou alebo právnickou osobou, ktorej bol certifikát vydaný;

39. „kvalifikovaný certifikát pre autentifikáciu webového sídla“ je certifikát pre autentifikáciu webového sídla, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe IV;

40. „validačné údaje“ sú údaje, ktoré sa používajú na validáciu elektronického podpisu, alebo elektronickej pečate;

41. „validácia“ je proces overenia a potvrdenia, že elektronický podpis alebo elektronická pečať sú platné.

Článok 4

Zásada vnútorného trhu

1. Poskytovanie dôveryhodných služieb na území členského štátu poskytovateľom dôveryhodných služieb usadeným v inom členskom štáte nemožno obmedziť z dôvodov, ktoré patria do oblastí, na ktoré sa vzťahuje toto nariadenie.

2. Na vnútornom trhu je povolený voľný obeh produktov a dôveryhodných služieb, ktoré sú v súlade s týmto nariadením.

Článok 5

Spracúvanie a ochrana údajov

1. Spracúvanie osobných údajov sa vykonáva v súlade so smernicou 95/46/ES.

2. Bez toho, aby bol dotknutý právny účinok pseudonymov podľa vnútroštátneho práva, nie je ich používanie pri elektronických transakciách zakázané.

KAPITOLA II

ELEKTRONICKÁ IDENTIFIKÁCIA

Článok 6

Vzájomné uznávanie

1. Keď sa podľa vnútroštátneho práva alebo administratívnej praxe na prístup k službe, ktorú poskytuje subjekt verejného sektora online v jednom členskom štáte, vyžaduje elektronická identifikácia pomocou prostriedkov elektronickej identifikácie a autentifikácia, prostriedky elektronickej identifikácie vydané v inom členskom štáte sa v prvom členskom štáte uznávajú na účely cezhraničnej autentifikácie pre danú službu online, ak sú splnené tieto podmienky:

a) prostriedky elektronickej identifikácie sa vydali v rámci schémy elektronickej identifikácie, ktorá je uvedená na zozname, ktorý Komisia uverejňuje podľa článku 9;

b) úroveň zabezpečenia prostriedkov elektronickej identifikácie zodpovedá úrovni zabezpečenia, ktorá je rovnaká alebo vyššia ako úroveň zabezpečenia, ktorú vyžaduje príslušný subjekt verejného sektora na prístup k danej službe online v prvom členskom štáte, za predpokladu, že úroveň zabezpečenia daných prostriedkov elektronickej identifikácie zodpovedá úrovni zabezpečenia „pokročilá“ alebo „vysoká“;

c) príslušný subjekt verejného sektora používa vo vzťahu k prístupu k danej službe online úroveň zabezpečenia „pokročilá“ alebo „vysoká“.

Takéto uznávanie sa začne najneskôr 12 mesiacov po tom, ako Komisia uverejní zoznam uvedený v písmene a) prvého pododseku.

2. Prostriedky elektronickej identifikácie vydané v rámci schémy elektronickej identifikácie, ktorá je uvedená na zozname, ktorý Komisia uverejňuje podľa článku 9, a ktoré zodpovedajú úrovni zabezpečenia „nízka“, môžu subjekty verejného sektora uznávať na účely cezhraničnej autentifikácie v prípade služieb, ktoré poskytujú online.

Článok 7

Podmienky pre oznamovanie schém elektronickej identifikácie

Schéma elektronickej identifikácie sa oznamuje podľa článku 9 ods. 1 za predpokladu, že sú splnené všetky tieto podmienky:

a) prostriedky elektronickej identifikácie v rámci schémy elektronickej identifikácie:

i) vydáva oznamujúci členský štát;

ii) sa vydávajú na základe poverenia oznamujúceho členského štátu alebo

iii) sa vydávajú nezávisle od oznamujúceho členského štátu, ktorý ich uznáva;

b) prostriedky elektronickej identifikácie v rámci schémy elektronickej identifikácie sa môžu použiť na prístup aspoň k jednej službe, ktorú poskytuje subjekt verejného sektora a ktorá vyžaduje elektronickú identifikáciu v oznamujúcom členskom štáte;

c) schéma elektronickej identifikácie a prostriedky elektronickej identifikácie, ktoré sa v rámci nej vydávajú, spĺňajú požiadavky pre aspoň jednu z úrovní zabezpečenia stanovených vo vykonávacom akte uvedenom v článku 8 ods. 3;

d) oznamujúci členský štát zabezpečuje, že osobné identifikačné údaje, ktoré jedinečne identifikujú dotknutú osobu, sa priraďujú v súlade s technickými špecifikáciami, normami a postupmi pre príslušnú úroveň zabezpečenia stanovenými vo vykonávacom akte uvedenom v článku 8 ods. 3 fyzickej alebo právnickej osobe uvedenej v článku 3 bode 1 v čase, keď sú prostriedky elektronickej identifikácie v rámci danej schémy vydané;

e) strana vydávajúca prostriedky elektronickej identifikácie v rámci danej schémy zabezpečuje, že prostriedky elektronickej identifikácie sa priradia osobe uvedenej v písmene d) tohto článku v súlade s technickými špecifikáciami, normami a postupmi pre príslušnú úroveň zabezpečenia stanovenými vo vykonávacom akte uvedenom v článku 8 ods. 3;

f) oznamujúci členský štát zabezpečuje dostupnosť autentifikácie online, aby ktorákoľvek spoliehajúca sa strana usadená na území iného členského štátu mohla potvrdiť osobné identifikačné údaje doručené v elektronickej forme.

Pre spoliehajúce sa strany, ktoré nie sú subjektmi verejného sektora, môže oznamujúci členský štát stanoviť podmienky prístupu k takejto autentifikácii. Cezhraničná autentifikácia sa poskytuje bezplatne, ak sa vykonáva vo vzťahu k službe online, ktorú poskytuje subjekt verejného sektora.

Členské štáty nesmú spoliehajúcim sa stranám, ktoré chcú vykonať takúto autentifikáciu, ukladať žiadne konkrétne neprimerané technické požiadavky, ak takéto požiadavky bránia alebo podstatne sťažujú interoperabilitu oznámených schém elektronickej identifikácie;

g) oznamujúci členský štát aspoň šesť mesiacov pred oznámením podľa článku 9 ods. 1 poskytne ostatným členským štátom na účely povinnosti podľa článku 12 ods. 5 opis danej schémy v súlade s dojednaniami o postupe stanovenými vo vykonávacích aktoch uvedených v článku 12 ods. 7;

h) schéma elektronickej identifikácie spĺňa požiadavky stanovené vo vykonávacom akte uvedenom v článku 12 ods. 8.

Článok 8

Úrovne zabezpečenia schém elektronickej identifikácie

1. Schéma elektronickej identifikácie oznámená podľa článku 9 ods. 1 obsahuje špecifikácie úrovní zabezpečenia „nízka“, „pokročilá“ a/alebo „vysoká“ pre prostriedky elektronickej identifikácie vydávané v rámci danej schémy.

2. Úrovne zabezpečenia „nízka“, „pokročilá“ a „vysoká“ spĺňajú tieto kritériá:

a) úroveň zabezpečenia „nízka“ sa vzťahuje na prostriedok elektronickej identifikácie v kontexte schémy elektronickej identifikácie, ktorý poskytuje obmedzený stupeň dôveryhodnosti, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, a je charakterizovaný odkazom na technické špecifikácie, normy a postupy vrátane technických kontrol, ktoré s ním súvisia a ktorých účelom je znížiť riziko zneužitia alebo pozmenenia totožnosti;

b) úroveň zabezpečenia „pokročilá“ sa vzťahuje na prostriedok elektronickej identifikácie v kontexte schémy elektronickej identifikácie, ktorý poskytuje pokročilý stupeň dôveryhodnosti, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, a je charakterizovaný odkazom na technické špecifikácie, normy a postupy vrátane technických kontrol, ktoré s ním súvisia a ktorých účelom je podstatne znížiť riziko zneužitia alebo pozmenenia totožnosti;

c) úroveň zabezpečenia „vysoká“ sa vzťahuje na prostriedok elektronickej identifikácie v kontexte schémy elektronickej identifikácie, ktorý poskytuje vyšší stupeň dôveryhodnosti ako prostriedok elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, a je charakterizovaný odkazom na technické špecifikácie, normy a postupy vrátane technických kontrol, ktoré s ním súvisia a ktorých účelom je zabrániť zneužitiu alebo pozmeneniu totožnosti.

3. S výhradou odseku 2 Komisia do 18. septembra 2015 prostredníctvom vykonávacích aktov stanoví minimálne technické špecifikácie, normy a postupy, na ktoré sa na účely odseku 1 odkazuje pri špecifikácii úrovní zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie, pričom zohľadní relevantné medzinárodné normy.

Uvedené minimálne technické špecifikácie, normy a postupy sa stanovia odkazom na spoľahlivosť a kvalitu týchto prvkov:

a) postup na preukázanie a overenie totožnosti fyzických alebo právnických osôb, ktoré žiadajú o vydanie prostriedku elektronickej identifikácie;

b) postup na vydanie požadovaného prostriedku elektronickej identifikácie;

c) mechanizmus autentifikácie, prostredníctvom ktorého fyzická alebo právnická osoba za použitia prostriedku elektronickej identifikácie potvrdzuje svoju totožnosť spoliehajúcej sa strane;

d) subjekt vydávajúci prostriedky elektronickej identifikácie;

e) akýkoľvek iný subjekt podieľajúci sa na žiadosti o vydanie prostriedku elektronickej identifikácie a

f) technické a bezpečnostné špecifikácie vydávaného prostriedku elektronickej identifikácie.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 9

Oznámenie

1. Oznamujúci členský štát oznámi Komisii nasledovné informácie a bez zbytočného odkladu všetky ich následné zmeny:

a) opis schémy elektronickej identifikácie vrátane jej úrovní zabezpečenia a vydavateľa alebo vydavateľov prostriedkov elektronickej identifikácie v schéme;

b) uplatniteľný režim dohľadu a informácie o režime zodpovednosti v súvislosti:

i) so stranou vydávajúcou prostriedky elektronickej identifikácie a

ii) so stranou realizujúcou postup autentifikácie;

c) orgán alebo orgány zodpovedné za schému elektronickej identifikácie;

d) informácie o subjekte alebo subjektoch, ktoré spravujú registráciu jedinečných osobných identifikačných údajov;

e) opis spôsobu plnenia požiadaviek stanovených vo vykonávacích aktoch uvedených v článku 12 ods. 8;

f) opis autentifikácie uvedenej v článku 7 písm. f);

g) dojednania týkajúce sa pozastavenia alebo zrušenia buď oznámenej schémy elektronickej identifikácie, alebo autentifikácie, alebo príslušných skompromitovaných častí.

2. Rok po dni začiatku uplatňovania vykonávacích aktov uvedených v článku 8 ods. 3 a článku 12 ods. 8 Komisia v *Úradnom vestníku Európskej únie* uverejní zoznam schém elektronickej identifikácie oznámených podľa odseku 1 tohto článku a základné informácie o nich.

3. Ak sa Komisii doručí oznámenie po uplynutí lehoty uvedenej v odseku 2, uverejní v *Úradnom vestníku Európskej únie* zmeny zoznamu uvedeného v odseku 2 do dvoch mesiacov odo dňa doručenia daného oznámenia.

4. Členský štát môže Komisii predložiť žiadosť o vypustenie schémy elektronickej identifikácie, ktorú oznámil, zo zoznamu uvedeného v odseku 2. Komisia uverejní v *Úradnom vestníku Európskej únie* príslušné zmeny zoznamu do jedného mesiaca odo dňa doručenia žiadosti členského štátu.

5. Komisia môže prostredníctvom vykonávacích aktov vymedziť okolnosti, formáty a postupy oznámení podľa odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 10

Narušenie bezpečnosti

1. Keď sa schéma elektronickej identifikácie oznámená podľa článku 9 ods. 1 alebo autentifikácia uvedená v článku 7 písm. f) naruší alebo čiastočne skompromituje spôsobom, ktorý ovplyvní spoľahlivosť cezhraničnej autentifikácie danej schémy, oznamujúci členský štát danú cezhraničnú autentifikáciu alebo dotknuté skompromitované časti bezodkladne pozastaví alebo zruší a informuje o tom ostatné členské štáty a Komisiu.

2. Po náprave narušenia alebo skompromitovania uvedeného v odseku 1 oznamujúci členský štát cezhraničnú autentifikáciu opätovne zavedie a bez zbytočného odkladu o tom informuje ostatné členské štáty a Komisiu.

3. Ak sa narušenie alebo skompromitovanie uvedené v odseku 1 neodstráni v lehote troch mesiacov od pozastavenia alebo zrušenia, oznamujúci členský štát informuje ostatné členské štáty a Komisiu o stiahnutí schémy elektronickej identifikácie.

Komisia bez zbytočného odkladu uverejní zodpovedajúce zmeny v zozname uvedenom v článku 9 ods. 2 v *Úradnom vestníku Európskej únie*.

Článok 11

Zodpovednosť

1. Oznamujúci členský štát je zodpovedný za škodu, ktorú spôsobí úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že pri cezhraničnej transakcii nesplní svoje povinnosti uvedené v článku 7 písm. d) a f).

2. Strana vydávajúca prostriedky elektronickej identifikácie je zodpovedná za škodu, ktorú spôsobí úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že pri cezhraničnej transakcii nesplní svoju povinnosť uvedenú v článku 7 písm. e).

3. Strana realizujúca postup autentifikácie je zodpovedná za škodu, ktorú spôsobí úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že pri cezhraničnej transakcii nezabezpečí správnu realizáciu autentifikácie uvedenú v článku 7 písm. f).

4. Odseky 1, 2 a 3 sa uplatňujú v súlade s vnútroštátnymi predpismi o zodpovednosti.

5. Odsekmi 1, 2 a 3 nie je dotknutá zodpovednosť strán transakcie podľa vnútroštátneho práva, pri ktorej sa používajú prostriedky elektronickej identifikácie patriace do schémy elektronickej identifikácie podľa článku 9 ods. 1.

Článok 12

Spolupráca a interoperabilita

1. Vnútroštátne schémy elektronickej identifikácie oznámené podľa článku 9 ods. 1 sú interoperabilné.

2. Na účely odseku 1 sa zavádza rámec interoperability.

3. Rámec interoperability musí spĺňať tieto kritériá:

a) jeho cieľom je technologická neutralita a neznevýhodňuje žiadne konkrétne vnútroštátne technické riešenie elektronickej identifikácie v rámci členského štátu;

b) podľa možností je v súlade s európskymi a medzinárodnými normami;

c) uľahčuje uplatňovanie zásady ochrany súkromia už v štádiu návrhu a

d) zabezpečuje sa ním, že osobné údaje sa spracúvajú v súlade so smernicou 95/46/ES.

4. Súčasťou rámca interoperability je:

a) odkaz na minimálne technické požiadavky týkajúce sa úrovní zabezpečenia podľa článku 8;

b) mapovanie vnútroštátnych úrovní zabezpečenia oznámených schém elektronickej identifikácie na úrovne zabezpečenia podľa článku 8;

c) odkaz na minimálne technické požiadavky týkajúce sa interoperability;

d) odkaz na minimálny súbor osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú alebo právnickú osobu, ktoré sú dostupné v schémach elektronickej identifikácie;

e) procedurálne predpisy;

f) mechanizmus urovnávania sporov a

g) spoločné normy prevádzkovej bezpečnosti.

5. Členské štáty spolupracujú, pokiaľ ide:

a) o interoperabilitu schém elektronickej identifikácie oznámených podľa článku 9 ods. 1 a schém elektronickej identifikácie, ktoré členské štáty zamýšľajú oznámiť, a

b) o bezpečnosť schém elektronickej identifikácie.

6. Spolupráca medzi členskými štátmi spočíva:

a) vo výmene informácií, skúseností a osvedčených postupov, pokiaľ ide o schémy elektronickej identifikácie, a najmä technické požiadavky týkajúce sa interoperability a úrovní zabezpečenia;

b) vo výmene informácií, skúseností a osvedčených postupov, pokiaľ ide o prácu s úrovňami zabezpečenia schém elektronickej identifikácie podľa článku 8;

c) v partnerskom preskúmaní schém elektronickej identifikácie, na ktoré sa vzťahuje toto nariadenie, a

d) v skúmaní príslušného vývoja v oblasti elektronickej identifikácie.

7. Komisia do 18. marca 2015 prostredníctvom vykonávacích aktov stanoví dojednania o postupoch potrebné na uľahčenie spolupráce medzi členskými štátmi uvedenej v odsekoch 5 a 6 s cieľom podporiť vysokú úroveň dôvery a bezpečnosti primeranú stupňu rizika.

8. Komisia na účely stanovenia jednotných podmienok vykonávania požiadavky podľa odseku 1, za splnenia kritérií stanovených v odseku 3 a zohľadňujúc výsledky spolupráce medzi členskými štátmi, prijme do 18. septembra 2015 vykonávacie akty o rámci interoperability, ako je stanovené v odseku 4.

9. Vykonávacie akty uvedené v odsekoch 7 a 8 tohto článku sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

KAPITOLA III

DÔVERYHODNÉ SLUŽBY

ODDIEL 1

Všeobecné ustanovenia

Článok 13

Zodpovednosť a dôkazné bremeno

1. Bez toho, aby bol dotknutý odsek 2, sú poskytovatelia dôveryhodných služieb zodpovední za škodu, ktorú spôsobia úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že nesplnia svoje povinnosti podľa tohto nariadenia.

Dôkazné bremeno týkajúce sa preukázania úmyslu alebo nedbanlivosti nekvalifikovaného poskytovateľa dôveryhodných služieb spočíva na fyzickej alebo právnickej osobe, ktorá žiada o náhradu škody uvedenej v prvom pododseku.

V prípade kvalifikovaného poskytovateľa dôveryhodných služieb sa škoda uvedená v prvom pododseku považuje za spôsobenú úmyselne alebo z nedbanlivosti, pokiaľ tento kvalifikovaný poskytovateľ dôveryhodných služieb nepreukáže opak.

2. Ak poskytovatelia dôveryhodných služieb svojim zákazníkom vopred riadne oznámia obmedzenia týkajúce sa využívania služieb, ktoré poskytujú, a ak tieto obmedzenia sú rozpoznateľné tretími stranami, poskytovatelia dôveryhodných služieb nenesú zodpovednosť za škody spôsobené využívaním služieb, ktorým sa takéto oznámené obmedzenia prekročili.

3. Odseky 1 a 2 sa uplatňujú v súlade s vnútroštátnymi predpismi o zodpovednosti.

Článok 14

Medzinárodné aspekty

1. Dôveryhodné služby, ktoré poskytujú poskytovatelia dôveryhodných služieb usadení v tretej krajine, sa uznávajú za právne rovnocenné s kvalifikovanými dôveryhodnými službami, ktoré poskytujú kvalifikovaní poskytovatelia dôveryhodných služieb usadení v Únii, ak sú dôveryhodné služby s pôvodom z tretej krajiny uznané dohodou uzavretou medzi Úniou a dotknutou treťou krajinou alebo medzinárodnou organizáciou v súlade s článkom 218 ZFEÚ.

2. Dohodami uvedenými v odseku 1 sa zabezpečuje najmä, že:

a) poskytovatelia dôveryhodných služieb z tretej krajiny alebo medzinárodné organizácie, s ktorými sa dohoda uzatvára, ako aj dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky uplatniteľné na kvalifikovaných poskytovateľov dôveryhodných služieb usadených v Únii a kvalifikované dôveryhodné služby, ktoré poskytujú;

b) kvalifikované dôveryhodné služby, ktoré poskytujú kvalifikovaní poskytovatelia dôveryhodných služieb usadení v Únii, sa uznávajú ako právne rovnocenné s dôveryhodnými službami, ktoré poskytujú poskytovatelia dôveryhodných služieb z tretích krajín alebo medzinárodné organizácie, s ktorými sa dohoda uzatvára.

Článok 15

Prístupnosť pre osoby so zdravotným postihnutím

Poskytované dôveryhodné služby a produkty pre koncových používateľov používané pri poskytovaní týchto služieb sú vždy, keď je to uskutočniteľné, prístupné osobám so zdravotným postihnutím.

Článok 16

Sankcie

Členské štáty stanovia pravidlá týkajúce sa sankcií uplatniteľných v prípade porušenia tohto nariadenia. Stanovené sankcie musia byť účinné, primerané a odrádzajúce.

ODDIEL 2

Dohľad

Článok 17

Orgán dohľadu

1. Členské štáty určia orgán dohľadu usadený na ich území alebo po vzájomnej dohode s iným členským štátom orgán dohľadu usadený v danom inom členskom štáte. Tento orgán je zodpovedný za úlohy dohľadu v určujúcom členskom štáte.

Orgánom dohľadu sa poskytnú potrebné právomoci a primerané zdroje na výkon ich úloh.

2. Členské štáty oznámia Komisii názvy a adresy svojich určených orgánov dohľadu.

3. Orgán dohľadu plní túto úlohu:

a) dohliada na kvalifikovaných poskytovateľov dôveryhodných služieb usadených na území určujúceho členského štátu s cieľom zaručiť prostredníctvom dohľadu *ex ante* a *ex post*, aby títo kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňali požiadavky stanovené v tomto nariadení;

b) podľa potreby koná prostredníctvom dohľadu *ex post* vo vzťahu k nekvalifikovaným poskytovateľom dôveryhodných služieb usadeným na území určujúceho členského štátu, ak má informácie, že títo nekvalifikovaní poskytovatelia dôveryhodných služieb alebo dôveryhodné služby, ktoré poskytujú, údajne nespĺňajú požiadavky stanovené v tomto nariadení.

4. Na účely odseku 3 a s výhradou obmedzení, ktoré sú v ňom ustanovené, medzi úlohy orgánu dohľadu patrí najmä:

a) spolupracovať s ostatnými orgánmi dohľadu a poskytovať im pomoc v súlade s článkom 18;

b) analyzovať správy o posudzovaní zhody uvedené v článku 20 ods. 1 a článku 21 ods. 1;

c) informovať ostatné orgány dohľadu a verejnosť o narušení bezpečnosti alebo integrity v súlade s článkom 19 ods. 2;

d) podávať Komisii správy o svojich hlavných činnostiach v súlade s odsekom 6 tohto článku;

e) vykonávať audity alebo žiadať orgán posudzovania zhody o posúdenie zhody týkajúce sa kvalifikovaných poskytovateľov dôveryhodných služieb v súlade s článkom 20 ods. 2;

f) spolupracovať s orgánmi pre ochranu osobných údajov a najmä ich bez zbytočného odkladu informovať o výsledkoch auditov kvalifikovaných poskytovateľov dôveryhodných služieb v prípade podozrenia z porušenia predpisov o ochrane osobných údajov;

g) udeľovať poskytovateľom dôveryhodných služieb a službám, ktoré poskytujú, kvalifikovaný štatút a odnímať ho v súlade s článkami 20 a 21;

h) informovať orgán zodpovedný za národný dôveryhodný zoznam uvedený v článku 22 ods. 3 o svojich rozhodnutiach týkajúcich sa udeľovania alebo odnímania kvalifikovaného štatútu, pokiaľ tento orgán nie je aj orgánom dohľadu;

i) overovať existenciu a správne uplatňovanie ustanovení o plánoch ukončenia činnosti v prípade, že kvalifikovaný poskytovateľ dôveryhodných služieb prestane vykonávať svoju činnosť, a to aj pokiaľ ide o spôsob, ako zachovať prístupnosť informácií v súlade s článkom 24 ods. 2 písm. h);

j) vyžadovať, aby poskytovatelia dôveryhodných služieb napravili akékoľvek nesplnenie požiadaviek stanovených v tomto nariadení.

5. Členské štáty môžu vyžadovať, aby orgán dohľadu zriadil, udržiaval a aktualizoval dôveryhodnú infraštruktúru v súlade s podmienkami podľa vnútroštátneho práva.

6. Všetky orgány dohľadu každoročne do 31. marca predložia Komisii správu o svojich hlavných činnostiach za predchádzajúci kalendárny rok spolu so súhrnom oznámení o narušeniach, ktoré dostali od poskytovateľov dôveryhodných služieb v súlade s článkom 19 ods. 2.

7. Komisia sprístupní výročnú správu uvedenú v odseku 6 členským štátom.

8. Komisia môže prostredníctvom vykonávacích aktov vymedziť formáty a postupy týkajúce sa správy uvedenej v odseku 6. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 18

Vzájomná pomoc

1. Orgány dohľadu navzájom spolupracujú s cieľom vymieňať si osvedčené postupy.

Orgán dohľadu poskytuje inému orgánu dohľadu na jeho odôvodnenú žiadosť pomoc, aby sa mohli činnosti orgánov dohľadu vykonávať konzistentným spôsobom. Vzájomná pomoc môže zahŕňať najmä žiadosti o informácie a opatrenia dohľadu, ako sú žiadosti o vykonanie inšpekcií súvisiacich so správami o posúdení zhody podľa článkov 20 a 21.

2. Orgán dohľadu, ktorému je adresovaná žiadosť o pomoc, môže túto žiadosť zamietnuť z ktoréhokoľvek z týchto dôvodov:

a) orgán dohľadu nie je na poskytnutie požadovanej pomoci príslušný;

b) požadovaná pomoc nie je primeraná činnostiam dohľadu, ktoré orgán dohľadu vykonáva v súlade s článkom 17;

c) poskytnutie požadovanej pomoci by nebolo v súlade s týmto nariadením.

3. Ak je to vhodné, členské štáty môžu oprávniť svoje orgány dohľadu na vykonávanie spoločných vyšetrovaní, do ktorých sa zapojí personál orgánov dohľadu z iných členských štátov. Dotknuté členské štáty dohodnú a ustanovia dojednania a postupy týkajúce sa takýchto spoločných akcií v súlade so svojím vnútroštátnym právom.

Článok 19

Bezpečnostné požiadavky uplatniteľné na poskytovateľov dôveryhodných služieb

1. Kvalifikovaní a nekvalifikovaní poskytovatelia dôveryhodných služieb prijmú vhodné technické a organizačné opatrenia na riadenie rizík ohrozujúcich bezpečnosť dôveryhodných služieb, ktoré poskytujú. So zreteľom na najnovší technologický vývoj sa uvedenými opatreniami musí zaistiť úroveň bezpečnosti primeraná stupňu rizika. Prijmú sa najmä opatrenia na prevenciu a minimalizáciu vplyvu bezpečnostných incidentov a na oznámenie nepriaznivých účinkov všetkých takýchto incidentov zainteresovaným stranám.

2. Kvalifikovaní a nekvalifikovaní poskytovatelia dôveryhodných služieb bez zbytočného odkladu, najneskôr však do 24 hodín, odkedy sa dozvedeli o akomkoľvek narušení bezpečnosti alebo integrity s významným vplyvom na poskytovanú dôveryhodnú službu alebo osobné údaje uchovávané v rámci nej, oznámia túto skutočnosť orgánu dohľadu a prípadne iným príslušným orgánom, ako je napríklad vnútroštátny orgán zodpovedný za informačnú bezpečnosť alebo orgán pre ochranu údajov.

Ak môže narušenie bezpečnosti alebo integrity negatívne ovplyvniť fyzickú alebo právnickú osobu, ktorej sa dôveryhodná služba poskytovala, poskytovateľ dôveryhodných služieb bez zbytočného odkladu oznámi narušenie bezpečnosti alebo integrity aj tejto fyzickej či právnickej osobe.

Ak je to vhodné, a najmä keď sa narušenie bezpečnosti alebo integrity týka dvoch alebo viacerých členských štátov, informovaný orgán dohľadu o veci informuje orgány dohľadu v ostatných dotknutých členských štátoch a agentúru ENISA.

Ak informovaný orgán dohľadu usúdi, že zverejnenie narušenia bezpečnosti alebo integrity je vo verejnom záujme, informuje o ňom verejnosť, alebo o to požiada poskytovateľa dôveryhodných služieb.

3. Orgán dohľadu poskytuje agentúre ENISA raz ročne súhrn oznámení o narušeniach bezpečnosti a integrity, ktoré mu oznámili poskytovatelia dôveryhodných služieb.

4. Komisia môže prostredníctvom vykonávacích aktov:

a) ďalej špecifikovať opatrenia uvedené v odseku 1 a

b) vymedziť formáty a postupy vrátane lehôt uplatniteľné na účely odseku 2.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

ODDIEL 3

Kvalifikované dôveryhodné služby

Článok 20

Dohľad nad kvalifikovanými poskytovateľmi dôveryhodných služieb

1. Orgán posudzovania zhody vykonáva aspoň každých 24 mesiacov audity kvalifikovaných poskytovateľov dôveryhodných služieb na ich vlastné náklady. Účelom auditu je potvrdiť, že kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v tomto nariadení. Kvalifikovaní poskytovatelia dôveryhodných služieb predložia výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

2. Bez toho, aby bol dotknutý odsek 1, môže orgán dohľadu kedykoľvek vykonať audit kvalifikovaných poskytovateľov dôveryhodných služieb alebo požiadať orgán posudzovania zhody, aby vykonal posúdenie zhody týkajúce sa kvalifikovaných poskytovateľov dôveryhodných služieb, a to na náklady týchto poskytovateľov dôveryhodných služieb, s cieľom potvrdiť, že títo poskytovatelia a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v tomto nariadení. Ak sa zdá, že boli porušené predpisy týkajúce sa ochrany osobných údajov, orgán dohľadu informuje o výsledkoch svojho auditu orgány pre ochranu údajov.

3. Ak orgán dohľadu vyžaduje od kvalifikovaného poskytovateľa dôveryhodných služieb nápravu akéhokoľvek nesplnenia požiadaviek podľa tohto nariadenia a ak tento poskytovateľ tak neurobí a ani počas prípadnej lehoty stanovenej orgánom dohľadu, orgán dohľadu pri zohľadnení najmä rozsahu, trvania a následkov takéhoto nesplnenia môže tomuto poskytovateľovi alebo dotknutej službe, ktorú poskytuje, odňať kvalifikovaný štatút a informovať o tom orgán uvedený v článku 22 ods. 3 na účely aktualizácie dôveryhodných zoznamov uvedených v článku 22 ods. 1. Orgán dohľadu informuje kvalifikovaného poskytovateľa dôveryhodných služieb o odňatí jeho kvalifikovaného štatútu alebo kvalifikovaného štatútu dotknutej služby.

4. Komisia môže prostredníctvom vykonávacích aktov stanoviť referenčné číslo týchto noriem:

a) akreditácia orgánov posudzovania zhody a správa o posúdení zhody uvedená v odseku 1;

b) pravidlá auditu, podľa ktorých orgány posudzovania zhody budú vykonávať posudzovanie zhody kvalifikovaných poskytovateľov dôveryhodných služieb podľa odseku 1.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 21

Začatie poskytovania kvalifikovanej dôveryhodnej služby

1. Ak poskytovatelia dôveryhodných služieb bez kvalifikovaného štatútu zamýšľajú začať poskytovať kvalifikované dôveryhodné služby, predložia orgánu dohľadu oznámenie o svojom zámere spolu so správou o posúdení zhody, ktorú vydal orgán posudzovania zhody.

2. Orgán dohľadu overí, či poskytovateľ dôveryhodných služieb a dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v tomto nariadení, a to najmä požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú.

Ak orgán dohľadu usúdi, že poskytovateľ dôveryhodných služieb a dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky uvedené v prvom pododseku, udelí tomuto poskytovateľovi dôveryhodných služieb a dôveryhodným službám, ktoré poskytuje, kvalifikovaný štatút a informuje orgán uvedený v článku 22 ods. 3 na účely aktualizácie dôveryhodných zoznamov uvedených v článku 22 ods. 1, a to najneskôr do troch mesiacov po oznámení v súlade s odsekom 1 tohto článku.

Ak sa overovanie neukončí do troch mesiacov od oznámenia, orgán dohľadu o tom informuje poskytovateľa dôveryhodných služieb a oznámi mu dôvody omeškania a lehotu, v ktorej sa overovanie má ukončiť.

3. Kvalifikovaní poskytovatelia dôveryhodných služieb môžu začať poskytovať kvalifikovanú dôveryhodnú službu po tom, čo sa kvalifikovaný štatút uvedie v dôveryhodných zoznamoch uvedených v článku 22 ods. 1.

4. Komisia môže prostredníctvom vykonávacích aktov vymedziť formáty a postupy na účely odsekov 1 a 2. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 22

Dôveryhodné zoznamy

1. Každý členský štát vytvorí, vedie a uverejňuje dôveryhodné zoznamy vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb, pre ktorých je príslušný, spolu s informáciami týkajúcimi sa kvalifikovaných dôveryhodných služieb, ktoré poskytujú.

2. Členské štáty zabezpečeným spôsobom vytvoria, vedú a uverejňujú elektronicky podpísané alebo zapečatené dôveryhodné zoznamy uvedené v odseku 1 vo forme vhodnej na automatizované spracovanie.

3. Členské štáty poskytnú Komisii bez zbytočného odkladu informácie o orgáne zodpovednom za vytvorenie, vedenie a uverejňovanie národných dôveryhodných zoznamov, ako aj údaje o tom, kde sa tieto zoznamy uverejňujú, informácie o certifikátoch použitých na podpísanie alebo zapečatenie dôveryhodných zoznamov a oznámia jej všetky ich zmeny.

4. Komisia prostredníctvom zabezpečeného kanálu sprístupňuje verejnosti informácie uvedené v odseku 3 v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

5. Komisia do 18. septembra 2015 prostredníctvom vykonávacích aktov spresní informácie uvedené v odseku 1 a vymedzí technické špecifikácie a formáty pre dôveryhodné zoznamy uplatniteľné na účely odsekov 1 až 4. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 23

Značka dôvery EÚ pre kvalifikované dôveryhodné služby

1. Kvalifikovaní poskytovatelia dôveryhodných služieb môžu značku dôvery EÚ používať na jednoduché, rozpoznateľné a jasné označenie kvalifikovaných dôveryhodných služieb, ktoré poskytujú po tom, čo sa kvalifikovaný štatút uvedený v článku 21 ods. 2 druhom pododseku uvedie v dôveryhodnom zozname uvedenom v článku 22 ods. 1.

2. Kvalifikovaní poskytovatelia dôveryhodných služieb pri používaní značky dôvery EÚ pre kvalifikované dôveryhodné služby uvedenej v odseku 1 zaručia, aby sa na ich webovom sídle uvádzal odkaz na príslušný dôveryhodný zoznam.

3. Komisia do 1. júla 2015 prostredníctvom vykonávacích aktov stanoví špecifikácie týkajúce sa formy, a najmä prezentáciu, kompozíciu, veľkosť a dizajn značky dôvery EÚ pre kvalifikované dôveryhodné služby. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 24

Požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb

1. Kvalifikovaný poskytovateľ dôveryhodných služieb pri vydávaní kvalifikovaného certifikátu pre dôveryhodnú službu vhodnými prostriedkami a v súlade s vnútroštátnym právom overuje totožnosť a prípadne akékoľvek osobitné atribúty fyzickej alebo právnickej osoby, ktorej vydáva kvalifikovaný certifikát.

Informácie uvedené v prvom pododseku overuje kvalifikovaný poskytovateľ dôveryhodných služieb buď priamo, alebo prostredníctvom spoľahnutia sa na tretiu stranu v súlade s vnútroštátnym právom:

a) na základe fyzickej prítomnosti fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, alebo

b) na diaľku prostredníctvom prostriedkov elektronickej identifikácie, pre ktoré sa pred vydaním kvalifikovaného certifikátu zabezpečila fyzická prítomnosť fyzickej osoby alebo splnomocneného zástupcu právnickej osoby a ktoré spĺňajú požiadavky stanovené v článku 8, pokiaľ ide o úroveň zabezpečenia „pokročilá“ alebo „vysoká“, alebo

c) prostredníctvom certifikátu pre kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať vydaného v súlade s písmenom a) alebo b), alebo

d) prostredníctvom použitia iných metód identifikácie uznávaných na vnútroštátnej úrovni, ktorými sa poskytuje rovnocenné zabezpečenie, pokiaľ ide o spoľahlivosť, ako pri fyzickej prítomnosti. Rovnocenné zabezpečenie potvrdzuje orgán posudzovania zhody.

2. Kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý poskytuje kvalifikované dôveryhodné služby:

a) informuje orgán dohľadu o všetkých zmenách pri poskytovaní svojich kvalifikovaných dôveryhodných služieb a o zámere ukončiť tieto činnosti;

b) zamestnáva personál a prípadne subdodávateľov s potrebnou odbornosťou, spoľahlivosťou, skúsenosťami, kvalifikáciou a vhodnou odbornou prípravou týkajúcou sa predpisov v oblasti bezpečnosti a ochrany osobných údajov a uplatňuje administratívne a riadiace postupy, ktoré zodpovedajú európskym alebo medzinárodným normám;

c) v súvislosti s rizikom zodpovednosti za škodu v súlade s článkom 13 udržiava postačujúce finančné prostriedky a/alebo uzatvára vhodné poistenie zodpovednosti za škodu v súlade s vnútroštátnym právom;

d) pred uzavretím zmluvného vzťahu jednoznačne a vyčerpávajúco informuje každú osobu, ktorá chce využívať kvalifikovanú dôveryhodnú službu, o presných podmienkach využívania tejto služby vrátane obmedzení jej využívania;

e) používa dôveryhodné systémy a produkty chránené proti pozmeneniu a zabezpečí technickú bezpečnosť a spoľahlivosť procesov, ktoré podporujú;

f) používa dôveryhodné systémy na uchovávanie jemu poskytnutých údajov v overiteľnej forme tak, aby:

i) údaje boli verejne prístupné na vyhľadanie iba po získaní súhlasu osoby, ktorej sa týkajú;

ii) údaje mohli zadávať a uchovávané údaje meniť iba oprávnené osoby;

iii) údaje bolo možné skontrolovať z hľadiska ich pravosti;

g) prijíma vhodné opatrenia proti falšovaniu a krádeži údajov;

h) zaznamenáva a po primeranú dobu, a to aj po ukončení činností kvalifikovaného poskytovateľa dôveryhodných služieb, uchováva prístupné všetky relevantné informácie týkajúce sa údajov, ktoré kvalifikovaný poskytovateľ dôveryhodných služieb vydal a prijal, najmä na účely predloženia dôkazov v súdnom konaní a na účely zabezpečenia kontinuity služby. Takéto zaznamenávanie sa môže vykonať elektronicky;

i) má aktualizovaný plán ukončenia činností na zabezpečenie kontinuity služby v súlade s ustanoveniami overenými orgánom dohľadu podľa článku 17 ods. 4 písm. i);

j) zabezpečí spracúvanie osobných údajov v súlade s právnymi predpismi podľa smernice 95/46/ES;

k) v prípade kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty, zriaďuje a aktualizuje databázu certifikátov.

3. Ak sa kvalifikovaný poskytovateľ dôveryhodných služieb vydávajúci kvalifikované certifikáty rozhodne certifikát zrušiť, zaznamená takéto zrušenie vo svojej databáze certifikátov a štatút zrušenia certifikátu uverejní čo najskôr, a v každom prípade do 24 hodín od doručenia žiadosti. Zrušenie je účinné ihneď po jeho uverejnení.

4. Pokiaľ ide o odsek 3, kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty, každej spoliehajúcej sa strane poskytnú informácie o štatúte platnosti alebo zrušenia kvalifikovaných certifikátov, ktoré vydali. Tieto informácie sa poskytujú aspoň, pokiaľ ide o jednotlivé certifikáty, kedykoľvek, a to aj po uplynutí doby platnosti certifikátu, automatizovaným spôsobom, ktorý je spoľahlivý, bezplatný a efektívny.

5. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre dôveryhodné systémy a produkty, ktoré sú v súlade s požiadavkami podľa odseku 2 písm. e) a f) tohto článku. Ak dôveryhodné systémy a produkty spĺňajú uvedené normy, má sa za to, že sú v súlade s požiadavkami stanovenými v tomto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

ODDIEL 4

Elektronické podpisy

Článok 25

Právne účinky elektronických podpisov

1. Právny účinok elektronického podpisu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že má elektronickú formu alebo že nespĺňa požiadavky pre kvalifikované elektronické podpisy.

2. Kvalifikovaný elektronický podpis má právny účinok rovnocenný s vlastnoručným podpisom.

3. Kvalifikovaný elektronický podpis založený na kvalifikovanom certifikáte vydanom v jednom členskom štáte sa uznáva ako kvalifikovaný elektronický podpis vo všetkých ostatných členských štátoch.

Článok 26

Požiadavky na zdokonalené elektronické podpisy

Zdokonalený elektronický podpis musí spĺňať tieto požiadavky:

a) je jedinečne spojený s podpisovateľom;

b) umožňuje určenie totožnosti podpisovateľa;

c) je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou, a

d) je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.

Článok 27

Elektronické podpisy vo verejných službách

1. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, vyžaduje zdokonalený elektronický podpis, uznáva tento členský štát zdokonalené elektronické podpisy, zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte pre elektronické podpisy a kvalifikované elektronické podpisy, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.

2. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, vyžaduje zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, uznáva tento členský štát zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte a kvalifikované elektronické podpisy, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.

3. Členské štáty nesmú vyžadovať na cezhraničné využívanie služby online, ktorú ponúka subjekt verejného sektora, elektronický podpis vyššej úrovne bezpečnosti ako kvalifikovaný elektronický podpis.

4. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre zdokonalené elektronické podpisy. Ak zdokonalený elektronický podpis spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami na zdokonalené elektronické podpisy uvedenými v odsekoch 1 a 2 tohto článku a v článku 26. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

5. Komisia do 18. septembra 2015 prostredníctvom vykonávacích aktov vymedzí referenčné formáty zdokonalených elektronických podpisov alebo referenčné metódy pre prípady, keď sa používajú alternatívne formáty, pričom zohľadní existujúcu prax, normy a právne akty Únie. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 28

Kvalifikované certifikáty pre elektronické podpisy

1. Kvalifikované certifikáty pre elektronické podpisy musia spĺňať požiadavky stanovené v prílohe I.

2. Kvalifikované certifikáty pre elektronické podpisy nesmú podliehať žiadnym povinným požiadavkám nad rámec požiadaviek stanovených v prílohe I.

3. Kvalifikované certifikáty pre elektronické podpisy môžu obsahovať nepovinné dodatočné osobitné atribúty. Uvedené atribúty nesmú mať vplyv na interoperabilitu a uznávanie kvalifikovaných elektronických podpisov.

4. Ak sa po počiatočnej aktivácii kvalifikovaný certifikát pre elektronické podpisy zruší, stráca svoju platnosť okamihom jeho zrušenia a jeho štatút sa za žiadnych okolností nezmení na pôvodný.

5. Členské štáty môžu ustanoviť vnútroštátne predpisy o dočasnom pozastavení kvalifikovaného certifikátu pre elektronický podpis, a to za týchto podmienok:

a) ak sa kvalifikovaný certifikát pre elektronický podpis dočasne pozastaví, certifikát stráca platnosť na obdobie pozastavenia;

b) obdobie pozastavenia sa jasne uvedie v databáze certifikátov a štatút pozastavenia musí byť počas obdobia pozastavenia viditeľný zo služby, ktorou sa poskytujú informácie o štatúte certifikátu.

6. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre kvalifikované certifikáty pre elektronický podpis. Ak kvalifikovaný certifikát pre elektronický podpis spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v prílohe I. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 29

Požiadavky na kvalifikované zariadenia na vyhotovenie elektronických podpisov

1. Kvalifikované zariadenia na vyhotovenie elektronických podpisov musia spĺňať požiadavky stanovené v prílohe II.

2. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre kvalifikované zariadenia na vyhotovenie elektronických podpisov. Ak kvalifikované zariadenie na vyhotovenie elektronického podpisu spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v prílohe II. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 30

Certifikácia kvalifikovaných zariadení na vyhotovenie elektronických podpisov

1. Zhodu kvalifikovaných zariadení na vyhotovenie elektronických podpisov s požiadavkami stanovenými v prílohe II certifikujú príslušné verejné alebo súkromné subjekty určené členskými štátmi.

2. Členské štáty oznámia Komisii názvy a adresy verejných alebo súkromných subjektov, ktoré sú uvedené v odseku 1. Komisia sprístupní tieto informácie členským štátom.

3. Certifikácia uvedená v odseku 1 je založená na:

a) procese hodnotenia bezpečnosti, ktorý sa vykoná v súlade s niektorou z noriem posudzovania bezpečnosti produktov informačných technológií zaradených do zoznamu vypracovaného v súlade s druhým pododsekom, alebo

b) inom procese ako procese uvedenom v písmene a), ak sa v rámci neho používajú porovnateľné úrovne bezpečnosti a ak verejný alebo súkromný subjekt uvedený v odseku 1 tento proces oznámi Komisii. Tento proces možno použiť, len ak neexistujú normy uvedené v písmene a) alebo ak prebieha proces hodnotenia bezpečnosti uvedený v písmene a).

Komisia prostredníctvom vykonávacích aktov vypracuje zoznam noriem posudzovania bezpečnosti produktov informačných technológií uvedený v písmene a). Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

4. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 47, pokiaľ ide o stanovenie osobitných kritérií, ktoré musia splniť určené subjekty uvedené v odseku 1 tohto článku.

Článok 31

Zverejňovanie zoznamu certifikovaných kvalifikovaných zariadení na vyhotovenie elektronických podpisov

1. Členské štáty bez zbytočného odkladu a najneskôr do jedného mesiaca po ukončení certifikácie poskytnú Komisii informácie o kvalifikovaných zariadeniach na vyhotovenie elektronických podpisov, ktoré certifikovali subjekty uvedené v článku 30 ods. 1. Rovnako bez zbytočného odkladu a najneskôr do jedného mesiaca po zrušení certifikácie poskytnú Komisii informácie o zariadeniach na vyhotovenie elektronických podpisov, ktoré už nie sú certifikované.

2. Komisia na základe získaných informácií vytvorí, zverejňuje a vedie zoznam certifikovaných kvalifikovaných zariadení na vyhotovenie elektronických podpisov.

3. Komisia môže prostredníctvom vykonávacích aktov vymedziť formáty a postupy uplatniteľné na účely odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 32

Požiadavky na validáciu kvalifikovaných elektronických podpisov

1. Procesom validácie kvalifikovaného elektronického podpisu sa potvrdí platnosť kvalifikovaného elektronického podpisu, ak:

a) certifikát, ktorý potvrdzuje podpis, bol v čase podpísania kvalifikovaným certifikátom pre elektronický podpis v súlade s prílohou I;

b) kvalifikovaný certifikát vydal kvalifikovaný poskytovateľ dôveryhodných služieb a v čase podpísania bol platný;

c) údaje na validáciu podpisu zodpovedajú údajom poskytnutým spoliehajúcej sa strane;

d) sa jedinečný súbor údajov reprezentujúcich podpisovateľa v certifikáte správne poskytol spoliehajúcej sa strane;

e) sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase podpísania použil pseudonym;

f) bol elektronický podpis vyhotovený kvalifikovaným zariadením na vyhotovenie elektronického podpisu;

g) nebola narušená integrita podpísaných údajov;

h) v čase podpísania boli dodržané požiadavky stanovené v článku 26.

2. Systém použitý na validáciu kvalifikovaného elektronického podpisu poskytuje spoliehajúcej sa strane správny výsledok procesu validácie a umožňuje spoliehajúcej sa strane odhaliť akékoľvek problémy súvisiace s bezpečnosťou.

3. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre validáciu kvalifikovaných elektronických podpisov. Ak validácia kvalifikovaných elektronických podpisov spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 33

Kvalifikovaná služba validácie kvalifikovaných elektronických podpisov

1. Kvalifikovanú službu validácie kvalifikovaných elektronických podpisov môže poskytovať iba kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý:

a) poskytuje validáciu v súlade s článkom 32 ods. 1 a

b) spoliehajúcim sa stranám umožňuje získať výsledok procesu validácie automatizovaným spôsobom, ktorý je spoľahlivý, efektívny a ktorý obsahuje zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať poskytovateľa kvalifikovanej služby validácie.

2. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre kvalifikovanú službu validácie uvedenú v odseku 1. Ak služba validácie kvalifikovaných elektronických podpisov spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 34

Kvalifikovaná služba uchovávania kvalifikovaných elektronických podpisov

1. Kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov môže poskytovať iba kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý používa postupy a technológie, ktoré umožňujú predĺžiť dôveryhodnosť kvalifikovaného elektronického podpisu aj na obdobie po uplynutí technologickej platnosti.

2. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov. Ak dojednania o kvalifikovanej službe uchovávania kvalifikovaných elektronických podpisov spĺňajú uvedené normy, má sa za to, že sú v súlade s požiadavkami stanovenými v odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

ODDIEL 5

Elektronické pečate

Článok 35

Právne účinky elektronických pečatí

1. Právny účinok elektronickej pečate a jej prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z dôvodu, že má elektronickú formu alebo že nespĺňa požiadavky pre kvalifikované elektronické pečate.

2. Pri kvalifikovanej elektronickej pečati platí domnienka integrity údajov a správnosti pôvodu tých údajov, s ktorými je kvalifikovaná elektronická pečať spojená.

3. Kvalifikovaná elektronická pečať založená na kvalifikovanom certifikáte vydanom v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická pečať vo všetkých ostatných členských štátoch.

Článok 36

Požiadavky na zdokonalené elektronické pečate

Zdokonalená elektronická pečať musí spĺňať tieto požiadavky:

a) je jedinečne spojená s pôvodcom pečate;

b) umožňuje určenie totožnosti pôvodcu pečate;

c) je vyhotovená pomocou údajov na vyhotovenie elektronickej pečate, ktoré môže pôvodca pečate s vysokou mierou dôveryhodnosti pod jeho kontrolou používať na vyhotovenie elektronickej pečate, a

d) je prepojená s údajmi, na ktoré sa vzťahuje, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.

Článok 37

Elektronické pečate vo verejných službách

1. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v mene tohto subjektu, vyžaduje zdokonalenú elektronickú pečať, uznáva tento členský štát zdokonalené elektronické pečate, zdokonalené elektronické pečate založené na kvalifikovanom certifikáte pre elektronické pečate a kvalifikované elektronické pečate, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.

2. Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v mene tohto subjektu, vyžaduje zdokonalenú elektronickú pečať založenú na kvalifikovanom certifikáte, uznáva tento členský štát zdokonalené elektronické pečate založené na kvalifikovanom certifikáte a kvalifikované elektronické pečate, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.

3. Členské štáty nesmú vyžadovať na cezhraničné využívanie služby online, ktorú ponúka subjekt verejného sektora, elektronickú pečať vyššej úrovne bezpečnosti ako kvalifikovaná elektronická pečať.

4. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre zdokonalené elektronické pečate. Ak zdokonalená elektronická pečať spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami na zdokonalené elektronické pečate uvedenými v odsekoch 1 a 2 tohto článku a v článku 36. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

5. Komisia do 18. septembra 2015 vymedzí prostredníctvom vykonávacích aktov referenčné formáty zdokonalených elektronických pečatí alebo referenčné metódy pre prípady, keď sa používajú alternatívne formáty, pričom zohľadní existujúcu prax, normy a právne akty Únie. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 38

Kvalifikované certifikáty pre elektronické pečate

1. Kvalifikované certifikáty pre elektronické pečate musia spĺňať požiadavky stanovené v prílohe III.

2. Kvalifikované certifikáty pre elektronické pečate nesmú podliehať žiadnym povinným požiadavkám nad rámec požiadaviek stanovených v prílohe III.

3. Kvalifikované certifikáty pre elektronické pečate môžu obsahovať nepovinné dodatočné osobitné atribúty. Týmito atribútmi sa neovplyvní interoperabilita a uznávanie kvalifikovaných elektronických pečatí.

4. Ak sa po počiatočnej aktivácii kvalifikovaný certifikát pre elektronickú pečať zruší, stráca svoju platnosť okamihom zrušenia a jeho štatút sa za žiadnych okolností nezmení na pôvodný.

5. Členské štáty môžu ustanoviť vnútroštátne predpisy o dočasnom pozastavení kvalifikovaných certifikátov pre elektronické pečate, a to za týchto podmienok:

a) ak sa kvalifikovaný certifikát pre elektronickú pečať dočasne pozastaví, tento certifikát stráca platnosť na obdobie pozastavenia;

b) obdobie pozastavenia sa jasne uvedie v databáze certifikátov a štatút pozastavenia musí byť počas obdobia pozastavenia viditeľný zo služby, ktorou sa poskytujú informácie o štatúte certifikátu.

6. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre kvalifikované certifikáty pre elektronické pečate. Ak kvalifikovaný certifikát pre elektronickú pečať spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v prílohe III. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 39

Kvalifikované zariadenia na vyhotovenie elektronických pečatí

1. Článok 29 sa primerane uplatňuje na požiadavky na kvalifikované zariadenia na vyhotovenie elektronických pečatí.

2. Článok 30 sa primerane uplatňuje na certifikáciu kvalifikovaných zariadení na vyhotovenie elektronických pečatí.

3. Článok 31 sa primerane uplatňuje na uverejňovanie zoznamu certifikovaných kvalifikovaných zariadení na vyhotovenie elektronických pečatí.

Článok 40

Validácia a uchovávanie kvalifikovaných elektronických pečatí

Články 32, 33 a 34 sa uplatňujú primerane na validáciu a uchovávanie kvalifikovaných elektronických pečatí.

ODDIEL 6

Elektronické časové pečiatky

Článok 41

Právny účinok elektronických časových pečiatok

1. Právny účinok elektronickej časovej pečiatky a jej prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že má elektronickú formu alebo že nespĺňa požiadavky kvalifikovanej elektronickej časovej pečiatky.

2. Pri kvalifikovanej elektronickej časovej pečiatke platí domnienka správnosti dátumu a času, ktorý uvádza, a integrity údajov, s ktorými je dátum a čas spojený.

3. Kvalifikovaná elektronická časová pečiatka vydaná v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická časová pečiatka vo všetkých členských štátoch.

Článok 42

Požiadavky na kvalifikované elektronické časové pečiatky

1. Kvalifikovaná elektronická časová pečiatka spĺňa tieto požiadavky:

a) spája dátum a čas s údajmi spôsobom, ktorý v rozumnej miere zamedzuje možnosť nezistiteľnej zmeny údajov;

b) je založená na presnom zdroji času prepojenom s koordinovaným svetovým časom a

c) je podpísaná zdokonaleným elektronickým podpisom alebo zapečatená zdokonalenou elektronickou pečaťou kvalifikovaného poskytovateľa dôveryhodných služieb alebo rovnocennou metódou.

2. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre spojenie dátumu a času s údajmi a pre presné zdroje času. Ak spojenie dátumu a času s údajmi a presným zdrojom času spĺňajú uvedené normy, má sa za to, že sú v súlade s požiadavkami stanovenými v odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

ODDIEL 7

Elektronické doručovacie služby pre registrované zásielky

Článok 43

Právny účinok elektronickej doručovacej služby pre registrované zásielky

1. Právny účinok údajov, ktoré sa odošlú a doručia prostredníctvom elektronickej doručovacej služby pre registrované zásielky, a ich prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z dôvodu, že majú elektronickú formu alebo že nespĺňajú požiadavky na kvalifikovanú elektronickú doručovaciu službu pre registrované zásielky.

2. Pri údajoch, ktoré sa odošlú a doručia prostredníctvom kvalifikovanej elektronickej doručovacej služby pre registrované zásielky, platí domnienka ich integrity, odoslania údajov identifikovaným odosielateľom a ich doručenia identifikovanému adresátovi a správnosti dátumu a času ich odoslania a doručenia uvedených v kvalifikovanej elektronickej doručovacej službe pre registrované zásielky.

Článok 44

Požiadavky na kvalifikované elektronické doručovacie služby pre registrované zásielky

1. Kvalifikované elektronické doručovacie služby pre registrované zásielky musia spĺňať tieto požiadavky:

a) poskytuje ich jeden alebo viacerí kvalifikovaní poskytovatelia dôveryhodných služieb;

b) zabezpečujú identifikáciu odosielateľa s vysokou úrovňou spoľahlivosti;

c) zabezpečujú identifikáciu adresáta pred doručením údajov;

d) odosielanie a doručovanie údajov je zabezpečené zdokonaleným elektronickým podpisom alebo zdokonalenou elektronickou pečaťou kvalifikovaného poskytovateľa dôveryhodných služieb spôsobom, ktorým sa zamedzí možnosti nezistiteľnej zmeny údajov;

e) akákoľvek zmena údajov potrebná na účel odoslania alebo doručenia údajov sa jasne oznámi odosielateľovi a adresátovi údajov;

f) dátum a čas odoslania, doručenia a akejkoľvek zmeny údajov je označený kvalifikovanou elektronickou časovou pečiatkou.

V prípade prenosu údajov medzi dvomi alebo viacerými kvalifikovanými poskytovateľmi dôveryhodných služieb sa požiadavky uvedené v písmenách a) až f) vzťahujú na všetkých kvalifikovaných poskytovateľov dôveryhodných služieb.

2. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre procesy odosielania a doručovania údajov. Ak proces odosielania a doručovania údajov spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

ODDIEL 8

Autentifikácia webových sídiel

Článok 45

Požiadavky na kvalifikované certifikáty pre autentifikáciu webových sídiel

1. Kvalifikované certifikáty pre autentifikáciu webových sídiel musia spĺňať požiadavky stanovené v prílohe IV.

2. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre kvalifikované certifikáty pre autentifikáciu webových sídiel. Ak kvalifikovaný certifikát pre autentifikáciu webových sídiel spĺňa uvedené normy, má sa za to, že je v súlade s požiadavkami stanovenými v prílohe IV. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

KAPITOLA IV

ELEKTRONICKÉ DOKUMENTY

Článok 46

Právne účinky elektronických dokumentov

Právny účinok elektronického dokumentu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z dôvodu, že má elektronickú formu.

KAPITOLA V

DELEGOVANIE PRÁVOMOCI A VYKONÁVACIE USTANOVENIA

Článok 47

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Právomoc prijímať delegované akty uvedené v článku 30 ods. 4 sa Komisii udeľuje na dobu neurčitú od 17. septembra 2014.

3. Delegovanie právomocí uvedené v článku 30 ods. 4 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

4. Komisia oznamuje delegovaný akt hneď po prijatí súčasne Európskemu parlamentu a Rade.

5. Delegovaný akt prijatý podľa článku 30 ods. 4 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 48

Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

KAPITOLA VI

ZÁVEREČNÉ USTANOVENIA

Článok 49

Preskúmanie

Komisia preskúma uplatňovanie tohto nariadenia a podá o ňom správu Európskemu parlamentu a Rade najneskôr 1. júla 2020. Komisia vyhodnotí najmä, či je vhodné zmeniť rozsah pôsobnosti tohto nariadenia alebo jeho konkrétne ustanovenia vrátane článku 6, článku 7 písm. f) a článkov 34, 43, 44 a 45, pričom sa zohľadnia skúsenosti získané počas uplatňovania tohto nariadenia, ako aj vývoj v oblasti technológií, trhu a práva.

K správe uvedenej v prvom odseku sa v prípade potreby priložia legislatívne návrhy.

Komisia okrem toho každé štyri roky po správe uvedenej v prvom odseku podáva Európskemu parlamentu a Rade správu o pokroku pri plnení cieľov tohto nariadenia.

Článok 50

Zrušenie

1. Smernica 1999/93/ES sa zrušuje s účinnosťou od 1. júla 2016.

2. Odkazy na zrušenú smernicu sa považujú za odkazy na toto nariadenie.

Článok 51

Prechodné opatrenia

1. Bezpečné zariadenia na vyhotovenie podpisu, ktorých zhoda sa určila v súlade s článkom 3 ods. 4 smernice 1999/93/ES, sa podľa tohto nariadenia považujú za kvalifikované zariadenia na vyhotovenie elektronických podpisov.

2. Kvalifikované certifikáty vydané fyzickým osobám podľa smernice 1999/93/ES sa považujú za kvalifikované certifikáty pre elektronické podpisy podľa tohto nariadenia do uplynutia ich platnosti.

3. Poskytovateľ certifikačných služieb vydávajúci kvalifikované certifikáty podľa smernice 1999/93/ES čo najskôr, najneskôr však 1. júla 2017 predloží orgánu dohľadu správu o posúdení zhody. Do predloženia takejto správy o posúdení zhody a dokončenia jej posudzovania zo strany orgánu dohľadu sa takýto poskytovateľ certifikačných služieb považuje za kvalifikovaného poskytovateľa dôveryhodných služieb podľa tohto nariadenia.

4. Ak poskytovateľ certifikačných služieb vydávajúci kvalifikované certifikáty podľa smernice 1999/93/ES nepredloží orgánu dohľadu správu o posúdení zhody v lehote uvedenej v odseku 3, takýto poskytovateľ certifikačných služieb sa od 2. júla 2017 nebude považovať za kvalifikovaného poskytovateľa dôveryhodných služieb podľa tohto nariadenia.

Článok 52

Nadobudnutie účinnosti

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

2. Toto nariadenie sa uplatňuje od 1. júla 2016 okrem týchto ustanovení:

a) článok 8 ods. 3, článok 9 ods. 5, článok 12 ods. 2 až 9, článok 17 ods. 8, článok 19 ods. 4, článok 20 ods. 4, článok 21 ods. 4, článok 22 ods. 5, článok 23 ods. 3, článok 24 ods. 5, článok 27 ods. 4 a 5, článok 28 ods. 6, článok 29 ods. 2, článok 30 ods. 3 a 4, článok 31 ods. 3, článok 32 ods. 3, článok 33 ods. 2, článok 34 ods. 2, článok 37 ods. 4 a 5, článok 38 ods. 6, článok 42 ods. 2, článok 44 ods. 2, článok 45 ods. 2 a články 47 a 48 sa uplatňujú od 17. septembra 2014;

b) článok 7, článok 8 ods. 1 a 2, články 9, 10 a 11 a článok 12 ods. 1 sa uplatňujú odo dňa začiatku uplatňovania vykonávacích aktov uvedených v článku 8 ods. 3 a článku 12 ods. 8;

c) článok 6 sa uplatňuje po uplynutí troch rokov od dátumu začiatku uplatňovania vykonávacích aktov uvedených v článku 8 ods. 3 a článku 12 ods. 8.

3. Ak je oznámená schéma elektronickej identifikácie uvedená na zozname, ktorý uverejnila Komisia podľa článku 9 pred dátumom uvedeným v odseku 2 písm. c) tohto článku, prostriedky elektronickej identifikácie v rámci tejto schémy sa uznajú podľa článku 6 najneskôr do 12 mesiacov po uverejnení uvedenej schémy, nie však skôr ako v deň uvedený v odseku 2 písm. c) tohto článku.

4. Členský štát sa môže bez ohľadu na odsek 2 písm. c) tohto článku rozhodnúť, že na jeho území sa prostriedky elektronickej identifikácie v rámci schémy elektronickej identifikácie oznámenej zo strany iného členského štátu podľa článku 9 ods. 1 uznajú odo dňa začiatku uplatňovania vykonávacích aktov uvedených v článku 8 ods. 3 a článku 12 ods. 8. Dotknuté členské štáty informujú Komisiu. Komisia tieto informácie zverejní.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 23. júla 2014

Za Parlament	*Za Radu*
predseda	*predseda*
M. SCHULZ	S. GOZI

PRÍLOHA I

POŽIADAVKY NA KVALIFIKOVANÉ CERTIFIKÁTY PRE ELEKTRONICKÉ PODPISY

Kvalifikované certifikáty pre elektronické podpisy obsahujú:

a) označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný certifikát pre elektronický podpis;

b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, zahŕňajúci aspoň členský štát, v ktorom je tento poskytovateľ usadený, a

— v prípade právnickej osoby: názov a prípadné registračné číslo, ako sa uvádza v úradných záznamoch,

— v prípade fyzickej osoby: meno osoby;

c) aspoň meno podpisovateľa alebo pseudonym; ak sa použije pseudonym, musí to byť jasne uvedené;

d) údaje na validáciu elektronického podpisu, ktoré zodpovedajú údajom na vyhotovenie elektronického podpisu;

e) údaje o začiatku a konci obdobia platnosti certifikátu;

f) identifikačný kód certifikátu, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb;

g) zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať vydávajúceho kvalifikovaného poskytovateľa dôveryhodných služieb;

h) lokalitu, na ktorej je certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať podľa písmena g) dostupný bezplatne;

i) lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného certifikátu;

j) ak sa údaje na vyhotovenie elektronického podpisu súvisiace s údajmi na validáciu elektronického podpisu nachádzajú v kvalifikovanom zariadení na vyhotovenie elektronického podpisu, primerané uvedenie tejto skutočnosti, prinajmenšom vo forme vhodnej na automatizované spracovanie.

PRÍLOHA II

POŽIADAVKY NA KVALIFIKOVANÉ ZARIADENIA NA VYHOTOVENIE ELEKTRONICKÝCH PODPISOV

1. Kvalifikované zariadenia na vyhotovenie elektronických podpisov musia vhodnými technickými a procedurálnymi prostriedkami zabezpečovať prinajmenšom, aby:

   a) v primeranej miere bola zaručená dôvernosť údajov na vyhotovenie elektronického podpisu použitých na vyhotovenie elektronického podpisu;

   b) sa údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu mohli v praxi objaviť iba raz;

   c) údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu nebolo možné s primeranou úrovňou zabezpečenia odvodiť a elektronický podpis bol spoľahlivo chránený proti falšovaniu pomocou aktuálne dostupných technológií;

   d) oprávnený podpisovateľ mohol údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu spoľahlivo chrániť pred použitím inými osobami.

2. Kvalifikované zariadenia na vyhotovenie elektronických podpisov nesmú meniť údaje, ktoré sa majú podpísať, ani brániť, aby sa takéto údaje podpisovateľovi pred podpísaním zobrazili.

3. Generovať alebo spravovať údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môže výhradne kvalifikovaný poskytovateľ dôveryhodných služieb.

4. Bez toho, aby bol dotknutý bod 1 písm. d), kvalifikovaní poskytovatelia dôveryhodných služieb spravujúci údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môžu údaje na vyhotovenie elektronického podpisu duplikovať len na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:

   a) bezpečnosť duplikovaných súborov údajov musí byť na rovnakej úrovni ako v prípade pôvodných súborov údajov;

   b) počet duplikovaných súborov údajov nesmie prekročiť minimálne množstvo nevyhnutné na zabezpečenie kontinuity služby.

PRÍLOHA III

POŽIADAVKY NA KVALIFIKOVANÉ CERTIFIKÁTY PRE ELEKTRONICKÉ PEČATE

Kvalifikované certifikáty pre elektronické pečate obsahujú:

a) označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydal ako kvalifikovaný certifikát pre elektronickú pečať;

b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, zahŕňajúci aspoň členský štát, v ktorom je tento poskytovateľ usadený, a

— v prípade právnickej osoby: názov a prípadné registračné číslo, ako sa uvádza v úradných záznamoch,

— v prípade fyzickej osoby: meno osoby;

c) aspoň meno vyhotoviteľa pečate a prípadné registračné číslo, ako sa uvádza v úradných záznamoch;

d) údaje na validáciu elektronickej pečate, ktoré zodpovedajú údajom na vyhotovenie elektronickej pečate;

e) údaje o začiatku a konci obdobia platnosti certifikátu;

f) identifikačný kód certifikátu, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb;

g) zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať vydávajúceho kvalifikovaného poskytovateľa dôveryhodných služieb;

h) lokalitu, na ktorej je certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať podľa písmena g) dostupný bezplatne;

i) lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného certifikátu;

j) ak sa údaje na vyhotovenie elektronickej pečate súvisiace s údajmi na validáciu elektronickej pečate nachádzajú v kvalifikovanom zariadení na vyhotovenie elektronickej pečate, primerané uvedenie tejto skutočnosti, prinajmenšom vo forme vhodnej na automatizované spracovanie.

PRÍLOHA IV

POŽIADAVKY NA KVALIFIKOVANÉ CERTIFIKÁTY PRE AUTENTIFIKÁCIU WEBOVÝCH SÍDIEL

Kvalifikované certifikáty pre autentifikáciu webových sídiel obsahujú:

a) označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný certifikát pre autentifikáciu webových sídiel;

b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, zahŕňajúci aspoň členský štát, v ktorom je poskytovateľ usadený, a:

— v prípade právnickej osoby: názov a prípadné registračné číslo tak, ako sa uvádza v úradných záznamoch,

— v prípade fyzickej osoby: meno osoby;

c) v prípade fyzických osôb: aspoň meno osoby, ktorej sa certifikát vydal, alebo jej pseudonym. Ak sa používa pseudonym, táto skutočnosť sa musí jednoznačne uviesť;

v prípade právnických osôb: aspoň názov právnickej osoby, ktorej sa certifikát vydáva, a prípadne registračné číslo tak, ako sa uvádza v úradných záznamoch;

d) prvky adresy, prinajmenšom vrátane mesta a štátu, fyzickej alebo právnickej osoby, ktorej sa certifikát vydáva, a prípadne tak, ako sa uvádza v úradných záznamoch;

e) názvy domén prevádzkovaných fyzickou alebo právnickou osobou, ktorej sa certifikát vydáva;

f) údaje o začiatku a konci obdobia platnosti certifikátu;

g) identifikačný kód certifikátu, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb;

h) zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať vydávajúceho kvalifikovaného poskytovateľa dôveryhodných služieb;

i) lokalitu, na ktorej je certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať uvedené v písmene h) dostupný bezplatne;

j) lokalitu služieb súvisiacich so štatútom platnosti certifikátov, ktoré sa môžu využiť na zistenie štatútu platnosti kvalifikovaného certifikátu.