EURÓPSKA KOMISIA

V Bruseli 4. 6. 2012
COM(2012) 238 final

2012/0146 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

(Text s významom pre EHP)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

V tejto dôvodovej správe sa objasňuje navrhovaný právny rámec vyvinutý na posilnenie dôvery v elektronické transakcie na vnútornom trhu.

Vybudovanie dôvery v prostredí online je kľúčom k hospodárskemu rozvoju. V dôsledku nedostatku dôvery spotrebitelia, podniky a správne orgány váhajú s realizáciou elektronických transakcií a prijímaním nových služieb.

V *Digitálnej agende pre Európu*[1] sa identifikujú existujúce bariéry digitálneho vývoja Európy a navrhujú sa právne predpisy o elektronických podpisoch (kľúčové opatrenie 3) a vzájomnom uznávaní elektronickej identifikácie a autentifikácie (kľúčové opatrenie 16), ktorými sa vytvorí jasný právny rámec s cieľom eliminovať fragmentáciu a nedostatočnú interoperabilitu, posilniť digitálne občianstvo a predchádzať počítačovej kriminalite. Právne predpisy zabezpečujúce vzájomné uznávanie elektronickej identifikácie a autentifikácie v celej EÚ a revízia smernice o elektronických podpisoch sú zároveň kľúčovým opatrením *Aktu o jednotnom trhu*[2] na realizáciu jednotného digitálneho trhu. V *Pláne pre stabilitu a rast*[3] sa zdôrazňuje pre vývoj digitálneho hospodárstva kľúčová úloha budúceho spoločného právneho rámca pre vzájomné uznávanie a akceptovanie elektronickej identifikácie a autentifikácie naprieč hranicami.

Cieľom navrhovaného právneho rámca, ktorý tvorí *„nariadenie Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu“*, je umožniť bezpečné a plynulé elektronické interakcie medzi podnikmi, občanmi a verejnými orgánmi, čím sa zvýši účinnosť verejných a súkromných služieb online, elektronického podnikania a elektronického obchodu v EÚ.

Existujúce právne predpisy EÚ, konkrétne smernica 1999/93/ES o *„rámci Spoločenstva pre elektronické podpisy“*[4], sa v podstate vzťahuje iba na elektronické podpisy. Neexistuje všeobecný cezhraničný a medziodvetvový rámec EÚ pre bezpečné, dôveryhodné a ľahko použiteľné elektronické transakcie, ktorý by sa vzťahoval na elektronickú identifikáciu, autentifikáciu aj podpisy.

Cieľom je posilniť existujúce právne predpisy a rozšíriť ich o vzájomné uznávanie a akceptovanie oznámených systémov elektronickej identifikácie a ďalších základných súvisiacich elektronických dôveryhodných služieb na úrovni EÚ.

2. VÝSLEDKY KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENIE VPLYVU

Táto iniciatíva je výsledkom rozsiahlych konzultácií so zainteresovanými stranami o revízii súčasného právneho rámca pre elektronické podpisy, na ktorých Komisia zozbierala spätnú

[1] KOM(2010) 245 z 19.5.2010.
[2] KOM(2011) 206 v konečnom znení z 13.4.2011.
[3] KOM(2011) 669, 12.10.2011.
[4] Ú. v. ES L 13, 19.1.2000, s. 12.

väzbu od členských štátov, Európskeho parlamentu a ďalších zainteresovaných strán[5]. Verejné online konzultácie doplnil „testovací panel MSP“ s cieľom identifikovať špecifické názory a potreby MSP a iné cielené konzultácie so zainteresovanými stranami[6] [7]. Komisia ďalej zabezpečila vypracovanie niekoľkých štúdií týkajúcich sa elektronickej identifikácie, autentifikácie, podpisov a súvisiacich dôveryhodných služieb (eIAS).

Z konzultácií jasne vyplynulo, že veľká väčšina zainteresovaných strán sa zhodla na potrebe revidovať súčasný rámec, aby sa zaplnili medzery, ktoré zanechala smernica o elektronickom podpise. Podľa názoru účastníkov by sa tak poskytla lepšia odpoveď na výzvy, ktoré predstavuje rýchly vývoj nových technológií (najmä prístupu online a mobilného prístupu) a narastajúca globalizácia, a zároveň by sa zachovala technologická neutrálnosť právneho rámca.

Komisia v súlade so svojou politikou „lepšej právnej regulácie“ vykonala posúdenie vplyvu politických možností. Posúdili sa tri súbory politických možností, týkajúce sa postupne (1) rozsahu nového rámca, (2) právneho nástroja a (3) požadovanej úrovne dohľadu[8]. Dokázalo sa, že uprednostnená politická možnosť posilní právnu istotu, rozšíri koordináciu vnútroštátneho dohľadu, zabezpečí vzájomné uznávanie a akceptovanie systémov elektronickej identifikácie a začlení základné súvisiace dôveryhodné služby. Posúdením vplyvu sa dospelo k záveru, že v rámci tejto možnosti by sa dosiahlo značné zlepšenie právnej istoty, bezpečnosti a dôvery pri cezhraničných elektronických transakciách, čo by viedlo k menšej fragmentácii trhu.

3. PRÁVNE PRVKY NÁVRHU

3.1 Právny základ

Tento návrh je založený na článku 114 ZFEÚ, ktorý sa týka prijatia pravidiel na odstránenie prekážok fungovania vnútorného trhu. Občania, podniky a správne orgány budú môcť využívať vzájomné uznávanie a akceptovanie elektronickej identifikácie, autentifikácie, podpisov a ďalších dôveryhodných služieb naprieč hranicami, keď sú potrebné na prístup k elektronickým postupom alebo transakciám a ich realizáciu.

Nariadenie sa považuje za najvhodnejší právny nástroj. Priama uplatniteľnosť nariadenia podľa článku 288 ZFEÚ zníži právnu fragmentáciu a poskytne väčšiu právnu istotu zavedením harmonizovaného súboru základných pravidiel, čo prispeje k fungovaniu vnútorného trhu.

---

5 Podrobné informácie o konzultáciách nájdete na http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

6 Dňa 10.3.2011 sa zorganizoval seminár pre zainteresované strany so zástupcami verejného, súkromného a akademického sektora, na ktorom sa diskutovalo o tom, aké legislatívne opatrenia sú potrebné na riešenie budúcich výziev. Išlo o interaktívne fórum na výmenu názorov a zdôraznenie rôznych pozícií v súvislosti s otázkami, ktoré sa objavili vo verejných konzultáciách. Viaceré organizácie spontánne zaslali svoje stanoviská.

7 Konkrétne poľské predsedníctvo EÚ zorganizovalo stretnutie s členskými štátmi týkajúce sa elektronického podpisu, ktoré sa konalo vo Varšave 9.11.2011, a ďalšie stretnutie týkajúce sa elektronickej identifikácie, ktoré sa konalo v Poznani 17.11.2011. Dňa 25.1.2012 Komisia zvolala seminár s členskými štátmi, na ktorom sa diskutovalo o zvyšných otázkach elektronickej identifikácie, autentifikácie a podpisov.

8 V rámci prvého súboru sa preskúmali štyri možnosti: zrušiť smernicu o elektronickom podpise; bez politickej zmeny; posilniť právnu istotu, posilniť koordináciu národného dohľadu a zabezpečiť vzájomné uznávanie a akceptovanie elektronickej identifikácie v celej EÚ; a po štvrté, rozšíriť o určité súvisiace dôveryhodné služby. Druhý súbor pozostával z posúdenia pomerných predností príležitostí regulácie pomocou jedného alebo dvoch nástrojov a pomocou smernice alebo nariadenia. V rámci tretieho súboru sa skúmali možnosti, ktoré ponúka implementácia vnútroštátnych systémov dohľadu na základe spoločných základných požiadaviek na dohľad v porovnaní so systémom dohľadu na úrovni EÚ. S pomocou skupiny spájajúcej všetky zainteresované generálne riaditeľstvá Komisie sa každá politická možnosť posúdila z hľadiska jej efektívnosti pri dosiahnutí politických cieľov, jej hospodárskeho vplyvu na zainteresované strany (aj na rozpočet inštitúcií EÚ), jej sociálneho a environmentálneho vplyvu a jej účinku na administratívnu záťaž.

3.2 Subsidiarita a proporcionalita

Ak má byť akcia EÚ odôvodnená, musí sa dodržať zásada subsidiarity:

a) Nadnárodná povaha problému (skúška nevyhnutnosti)

Nadnárodná povaha služieb eIAS vyžaduje opatrenia na úrovni EÚ. Domáce (t. j. vnútroštátne) opatrenia by nestačili na dosiahnutie cieľov stanovených v *stratégii Európa 2020*[9]. Na druhej strane skúsenosti ukázali, že vnútroštátne opatrenia *de facto* vytvorili bariéry pre interoperabilitu elektronických podpisov v celej EÚ a v súčasnosti majú rovnaký účinok na elektronickú identifikáciu, elektronickú autentifikáciu a súvisiace dôveryhodné služby. Preto je nevyhnutné, aby sa v EÚ vytvoril uľahčujúci rámec, ktorým sa vyrieši cezhraničná interoperabilita a zlepšila koordinácia národných systémov dohľadu. Elektronická identifikácia sa však v navrhovanom nariadení nemôže riešiť rovnako všeobecným spôsobom ako ďalšie dôveryhodné elektronické služby, pretože vydávanie prostriedkov identifikácie je výsadou členských štátov. Návrh je preto zameraný striktne na cezhraničné aspekty elektronickej identifikácie.

Navrhované nariadenie vytvára rovnaké pravidlá hry pre podniky poskytujúce dôveryhodné služby tam, kde v súčasnosti existujúce rozdiely medzi vnútroštátnymi právnymi predpismi často vedú k neistote a dodatočnej záťaži. Právna istota sa významne zvyšuje pomocou jasných povinností akceptovania kvalifikovaných dôveryhodných služieb zo strany členských štátov, čím sa vytvorí ďalší stimul pre expandovanie podnikov do zahraničia. Spoločnosť sa napríklad bude môcť elektronicky zúčastniť na verejnej výzve na predloženie ponúk, ktorú vydá správny orgán iného členského štátu bez toho, aby bol jej elektronický podpis blokovaný pre osobitné vnútroštátne požiadavky a problémy s interoperabilitou. Podobne spoločnosť bude mať príležitosť podpisovať zmluvy elektronicky so zmluvným partnerom v inom členskom štáte bez toho, aby sa musela obávať odlišných právnych požiadaviek na dôveryhodné služby, ako sú elektronické pečate, elektronické dokumenty alebo časové pečiatky. A konečne, oznámenie o neplnení sa doručí z jedného členského štátu do druhého s istotou jeho právnej platnosti v oboch členských štátoch. Napokon, obchodovanie online bude dôveryhodnejšie, keď kupujúci budú mať prostriedky, ktorými si overia, že skutočne otvárajú webovú lokalitu obchodníka, ktorého si vybrali, a nie prípadnú falošnú webovú stránku.

Vzájomne uznávané prostriedky elektronickej identifikácie a široko akceptované elektronické podpisy uľahčia cezhraničné poskytovanie početných služieb na vnútornom trhu a umožnia podnikom expandovať do zahraničia bez toho, aby čelili prekážkam pri interakcii s orgánmi verejnej moci. V praxi to bude znamenať významné zlepšenie efektivity pre podniky aj pre občanov v rámci dodržiavania administratívnych formalít. Ponúkne sa napríklad príležitosť študentovi, aby sa elektronicky zapísal na univerzitu v zahraničí, občanovi, aby podal daňové priznanie online v inom členskom štáte, alebo pacientovi, aby mal prístup k svojim zdravotným údajom online. Ak nebudú existovať takéto vzájomne uznávané prostriedky elektronickej identifikácie, lekár nebude mať prístup k zdravotným záznamom pacienta, ktoré potrebuje na jeho liečbu, a klinické a laboratórne testy, ktoré už pacient podstúpil, sa budú musieť opakovať.

b) Pridaná hodnota (skúška efektívnosti)

[9] Oznámenie Komisie: Európa 2020. Stratégia na zabezpečenie inteligentného, udržateľného a inkluzívneho rastu, KOM(2010) 2020, 3.3.2010.

Uvedené ciele sa v súčasnosti nedarí dosiahnuť dobrovoľnou koordináciou medzi členskými štátmi, a nie je ani dostatočne pravdepodobné, že sa to podarí v budúcnosti. **To vedie** k zdvojovaniu úsilia, nastavovaniu rozdielnych noriem, nadnárodných charakteristík externalít vyprodukovaných IKT a administratívnej zložitosti zavedenia takejto koordinácie prostredníctvom dvojstranných a multilaterálnych dohôd.

Navyše potreba prekonať také problémy, ako sú a) absencia právnej istoty pre heterogénne národné ustanovenia pochádzajúce z rozdielnych výkladov smernice o elektronickom podpise a b) nedostatočná interoperabilita systémov elektronického podpisu vytvorených na vnútroštátnej úrovni pre nejednotné uplatňovanie technických noriem, si vyžaduje taký druh koordinácie medzi členskými štátmi EÚ, ktorý je možné efektívnejšie realizovať na úrovni EÚ.

3.3 Podrobné vysvetlenie návrhu

3.3.1 KAPITOLA I – VŠEOBECNÉ USTANOVENIA

V článku 1 sa vymedzuje predmet úpravy nariadenia.

V článku 2 sa vymedzuje vecný rozsah pôsobnosti nariadenia.

V článku 3 sa uvádzajú definície termínov používaných v nariadení. Hoci niektoré definície sú prevzaté zo smernice 1999/93/ES, iné sú vysvetlené, doplnené ďalšími prvkami alebo novo zavedené.

V článku 4 sa určujú zásady vnútorného trhu týkajúce sa územného uplatňovania nariadenia. Uvádza sa explicitná zmienka o nezavedení žiadnych obmedzení slobody poskytovania služieb a voľného obehu výrobkov.

3.3.2 KAPITOLA II – ELEKTRONICKÁ IDENTIFIKÁCIA

V článku 5 sa stanovuje vzájomné uznávanie a akceptovanie prostriedkov elektronickej identifikácie, ktoré patria do systému oznámeného Komisii za podmienok stanovených v nariadení. Väčšina členských štátov EÚ zaviedla určitú formu systému elektronickej identifikácie. Jednotlivé systémy sa však v mnohých aspektoch líšia. Neexistencia spoločného právneho základu, na základe ktorého by sa od každého členského štátu vyžadovalo, aby uznával a akceptoval prostriedky elektronickej identifikácie vydané v iných členských štátoch pri prístupe k službám online, spolu s neprimeranou cezhraničnou interoperabilitou národných elektronických identifikácií vytvára prekážky, ktoré občanom a podnikom bránia využívať digitálny jednotný trh. Vzájomným uznávaním a akceptovaním akýchkoľvek prostriedkov elektronickej identifikácie patriacej do oznámeného systému podľa tohto nariadenia sa tieto právne prekážky odstránia.

Nariadenie nezaväzuje členské štáty, aby zaviedli, alebo oznámili systémy elektronickej identifikácie, ale aby uznávali a akceptovali oznámené elektronické identifikácie v prípade služieb online, pri ktorých sa na prístup na vnútroštátnej úrovni vyžaduje elektronická identifikácia. Potenciálne zvýšenie úspor z rozsahu vytvorených vďaka cezhraničnému využívaniu oznámených prostriedkov elektronickej identifikácie a systémov autentifikácie môže stimulovať členské štáty, aby oznamovali svoje systémy elektronickej identifikácie. V článku 6 sa stanovuje päť podmienok oznámenia systémov elektronickej identifikácie:

Členské štáty môžu oznámiť systémy elektronickej identifikácie, ktoré akceptujú v rámci svojej jurisdikcie, keď sa pri verejných službách vyžaduje elektronická identifikácia. Ďalšia požiadavka spočíva v tom, že príslušný prostriedok identifikácie musí byť vydaný členským štátom, ktorý oznamuje daný systém, v jeho mene, alebo aspoň pod dohľadom tohto členského štátu.

Členské štáty musia zabezpečiť jednoznačné prepojenie medzi údajmi elektronickej identifikácie a príslušnou osobou. Táto povinnosť neznamená, že osoba nemôže mať viaceré prostriedky elektronickej identifikácie, ale že všetky tieto prostriedky musia byť spojené s tou istou osobou.

Spoľahlivosť elektronickej identifikácie závisí od dostupnosti prostriedkov autentifikácie (čiže možnosti overiť platnosť údajov slúžiacich na elektronickú identifikáciu). Nariadenie zaväzuje oznamujúce členské štáty, aby tretím stranám poskytovali bezplatnú autentifikáciu online. Možnosť autentifikácie musí byť dostupná nepretržite. Stranám spoliehajúcim sa na takúto autentifikáciu sa nemôžu ukladať žiadne konkrétne technické požiadavky, napríklad na hardvér alebo na softvér. Toto ustanovenie sa nevzťahuje na žiadne požiadavky voči používateľom (držiteľom) prostriedkov elektronickej identifikácie, ktoré sú technicky nevyhnutné na používanie prostriedkov elektronickej identifikácie, napríklad čítačky kariet.

Členské štáty musia prijať zodpovednosť za jednoznačnosť prepojenia (t. j. za to, že identifikačné údaje priradené osobe nesmú byť prepojené so žiadnou inou osobou) a možnosť autentifikácie (t. j. možnosť skontrolovať platnosť údajov elektronickej identifikácie). Zodpovednosť členských štátov sa nevzťahuje na ostatné aspekty identifikačného procesu, ani na ďalšie transakcie vyžadujúce identifikáciu.

Článok 7 obsahuje pravidlá oznamovania systémov elektronickej identifikácie Komisii.

Cieľom článku 8 je zabezpečiť technickú interoperabilitu oznámených systémov identifikácie pomocou koordinovaného prístupu vrátane delegovaných aktov.

3.3.3 KAPITOLA III – DÔVERYHODNÉ SLUŽBY

3.3.3.1 Oddiel 1 – Všeobecné ustanovenia

V článku 9 sa stanovujú zásady týkajúce sa zodpovednosti nekvalifikovaných a kvalifikovaných poskytovateľov dôveryhodných služieb. Zakladá sa na článku 6 smernice 1999/93/ES a rozširuje nárok na náhradu škody spôsobenej akýmkoľvek nedbanlivým poskytovateľom dôveryhodnej služby v dôsledku nedodržania osvedčených bezpečnostných postupov, ktorého výsledkom je narušenie bezpečnosti s významným vplyvom na službu.

V článku 10 sa opisuje mechanizmus uznávania a akceptovania kvalifikovaných dôveryhodných služieb poskytovaných poskytovateľom so sídlom v tretej krajine. Zakladá sa na článku 7 smernice 1999/93/ES, no zachováva iba jedinú v praxi reálnu možnosť, ktorou je umožniť takéto uznávanie v rámci medzinárodnej dohody medzi Európskou úniou a tretími krajinami alebo medzinárodnými organizáciami.

V článku 11 sa stanovujú zásady ochrany a minimalizácie údajov. Zakladá sa na článku 8 smernice 1999/93/ES.

V článku 12 sa stanovuje dostupnosť dôveryhodných služieb pre ľudí s postihnutím.

3.3.3.2 Oddiel 2 – Dohľad

V článku 13 sa členské štáty zaväzujú, aby vytvorili orgány dohľadu na základe článku 3 ods. 3 smernice 1999/93/ES, a vysvetľuje a rozširuje sa v ňom ich oblasť právomocí vo vzťahu tak k poskytovateľom dôveryhodných služieb, ako aj ku kvalifikovaným poskytovateľom dôveryhodných služieb.

V článku 14 sa zavádza explicitný mechanizmus vzájomnej pomoci medzi orgánmi dohľadu v členských štátoch s cieľom uľahčiť cezhraničný dohľad nad poskytovateľmi dôveryhodných služieb. Zavádzajú sa v ňom pravidlá spoločných operácií a právo orgánov dohľadu zúčastniť sa na takýchto operáciách.

V článku 15 sa zavádza povinnosť pre kvalifikovaných aj nekvalifikovaných poskytovateľov dôveryhodných služieb vykonať vhodné technické a organizačné opatrenia pre bezpečnosť ich činností. Navyše, každé narušenie bezpečnosti sa musí oznámiť orgánom dohľadu a iným príslušným orgánom. Ak je to vhodné, tieto orgány následne informujú orgány dohľadu ďalších členských štátov a priamo alebo prostredníctvom príslušného poskytovateľa dôveryhodných služieb informujú aj verejnosť.

V článku 16 sa stanovujú podmienky dohľadu nad kvalifikovanými poskytovateľmi dôveryhodných služieb. Zaväzuje kvalifikovaných poskytovateľov dôverných služieb, aby nezávislý subjekt každoročne vykonal audit ich služieb s cieľom potvrdiť orgánu dohľadu, že spĺňajú povinnosti stanovené v nariadení. V článku 16 ods. 2 sa orgánu dohľadu navyše udeľuje právo kedykoľvek vykonať audit kvalifikovaných poskytovateľov dôveryhodných služieb na mieste. Orgán dohľadu má ďalej právomoc vydať kvalifikovaným poskytovateľom dôveryhodných služieb záväzné pokyny na primeranú nápravu akéhokoľvek nedodržania povinnosti, ktoré odhalí bezpečnostný audit.

Článok 17 sa týka činnosti, ktorú vykonáva orgán dohľadu pri žiadosti poskytovateľa dôveryhodnej služby o začatie kvalifikovanej dôveryhodnej služby.

V článku 18 sa stanovuje vytvorenie zoznamov dôveryhodných informácií[10] obsahujúcich informácie o kvalifikovaných poskytovateľoch dôveryhodných služieb, ktorí podliehajú dohľadu, a o dôveryhodných službách, ktoré ponúkajú. Tieto informácie sa musia uverejniť prostredníctvom spoločného vzoru s cieľom uľahčiť ich automatické použitie a zabezpečiť vhodnú úroveň podrobnosti.

V článku 19 sa stanovujú požiadavky, ktoré musia splniť kvalifikovaní poskytovatelia dôveryhodných služieb, aby mohli byť uznaní ako kvalifikovaní. Vychádza z prílohy II k smernici 1999/93/ES.

3.3.3.3 Oddiel 3 – Elektronický podpis

V článku 20 sa stanovujú pravidlá týkajúce sa právneho účinku elektronických podpisov fyzických osôb. Vysvetľuje a rozširuje sa v ňom článok 5 smernice 1999/93/ES a zavádza sa explicitná povinnosť priznať kvalifikovaným elektronickým podpisom rovnaký právny účinok ako vlastnoručným podpisom. Členské štáty musia navyše zabezpečiť cezhraničné akceptovanie kvalifikovaných elektronických podpisov v kontexte poskytovania verejných

[10] Základom pre nové rozhodnutie Komisie o zozname dôveryhodných informácií podľa tohto nariadenia, je zoznam dôveryhodných informácií ustanovený rozhodnutím Komisie 2009/767/ES, zmeneným a doplneným rozhodnutím Komisie 2010/425/EÚ.

služieb a nesmú zaviesť žiadne dodatočné požiadavky, ktoré by mohli vytvoriť prekážky pre používanie takýchto podpisov.

V článku 21 sa stanovujú požiadavky na certifikáty kvalifikovaných podpisov. Vyjasňuje sa v ňom príloha I k smernici 1999/93/ES a odstraňujú sa ustanovenia, ktoré v praxi nefungovali (napríklad obmedzenia hodnoty transakcií).

V článku 22 sa stanovujú požiadavky na zariadenia na vytvorenie kvalifikovaného elektronického podpisu. Vyjasňujú sa v ňom požiadavky na bezpečné zariadenia na vytvorenie podpisu, stanovené v článku 3 ods. 5 smernice 1999/93/ES, ktoré sa odteraz musia považovať za zariadenia na vytvorenie kvalifikovaného podpisu podľa tohto nariadenia. Ďalej sa v ňom vyjasňuje, že rozsah zariadenia na vytvorenie podpisu môže byť oveľa širší ako iba niečo, čo obsahuje údaje na vytvorenie podpisu. Komisia môže vytvoriť aj zoznam referenčných čísel noriem pre bezpečnostné požiadavky kladené na zariadenia.

V článku 23, ktorý vychádza z článku 3 ods. 4 smernice 1999/93/ES, sa zavádza koncepcia certifikácie zariadení na kvalifikovaný elektronický podpis s cieľom určiť ich súlad s bezpečnostnými požiadavkami stanovenými v prílohe II. Počas výkonu certifikačného postupu certifikačným orgánom určeným členským štátom musia všetky členské štáty uznať tieto zariadenia ako zariadenia vyhovujúce stanoveným požiadavkám. Komisia uverejní pozitívny zoznam takýchto certifikovaných zariadení podľa článku 24. Komisia môže vytvoriť aj zoznam referenčných čísel noriem pre bezpečnostné posúdenie produktov informačných technológií, ako sa uvádza v článku 23 ods. 1.

Článok 24 sa týka zverejňovania zoznamu zariadení na vytvorenie kvalifikovaných elektronických podpisov Komisiou po oznámení súladu členskými štátmi.

Článok 25 vychádza z odporúčaní uvedených v prílohe IV k smernici 1999/93/ES stanoviť záväzné požiadavky na potvrdzovanie platnosti kvalifikovaných elektronických podpisov s cieľom zvýšiť právnu istotu takéhoto potvrdenia platnosti.

V článku 26 sa stanovujú podmienky kvalifikovaných služieb potvrdzovania platnosti.

V článku 27 sa stanovuje podmienka dlhodobého uchovávania kvalifikovaných elektronických podpisov. Je to možné vďaka využívaniu postupov a technológií, ktoré umožňujú rozšíriť dôveryhodnosť údajov slúžiacich na potvrdenie platnosti kvalifikovaného elektronického podpisu aj po uplynutí ich technologickej platnosti, keď už môže byť pre páchateľov počítačových trestných činov ľahké takýto podpis sfalšovať.

3.3.3.4 Oddiel 4 – Elektronické pečate

Článok 28 sa týka právneho účinku elektronických pečatí právnických osôb. Na kvalifikovanú elektronickú pečať sa vzťahuje osobitná právna domnienka, ktorá zaručuje pôvod a neporušenosť elektronických dokumentov, s ktorými je spojená.

V článku 29 sa stanovujú požiadavky na kvalifikované certifikáty elektronických pečatí.

V článku 30 sa stanovujú požiadavky na zoznam zariadení na vytvorenie kvalifikovanej elektronickej pečate, ako aj jeho certifikácia a zverejňovanie.

V článku 31 sa stanovuje podmienka potvrdzovania platnosti a uchovávania kvalifikovaných elektronických pečatí.

3.3.3.5 Oddiel 5 – Elektronická časová pečiatka

Článok 32 sa týka právneho účinku elektronických časových pečiatok. Na kvalifikované elektronické časové pečiatky sa vzťahuje osobitná právna domnienka v súvislosti s istotou času.

V článku 33 sa stanovujú požiadavky na kvalifikované elektronické časové pečiatky.

3.3.3.6 Oddiel 6 – Elektronické dokumenty

Článok 34 súvisí s právnymi účinkami a podmienkami akceptovania elektronických dokumentov. Na akýkoľvek elektronický dokument podpísaný kvalifikovaným elektronickým podpisom alebo označený kvalifikovanou elektronickou pečaťou sa vzťahuje osobitná právna domnienka o jeho pravosti a neporušenosti. Pokiaľ ide o akceptovanie elektronických dokumentov, keď sa na poskytnutie verejnej služby vyžaduje originálny dokument alebo certifikovaná kópia, prinajmenšom elektronické dokumenty vydané osobami, ktoré majú právomoc vydávať príslušné dokumenty a ktoré sa považujú za originály alebo certifikované kópie v súlade s vnútroštátnymi právnymi predpismi členského štátu pôvodu, sa akceptujú v iných členských štátoch bez dodatočných požiadaviek.

3.3.3.7 Oddiel 7 – Elektronické doručovacie služby

Článok 35 sa týka právneho účinku údajov odoslaných alebo prijatých pomocou elektronickej doručovacej služby. Na kvalifikované elektronické doručovacie služby sa vzťahuje osobitná právna domnienka týkajúca sa neporušenosti odosielaných alebo prijímaných údajov a presnosti času odoslania alebo prijatia údajov. Zároveň sa zabezpečuje vzájomné uznávanie kvalifikovaných elektronických doručovacích služieb na úrovni EÚ.

V článku 36 sa stanovujú požiadavky na kvalifikované elektronické doručovacie služby.

3.3.3.8 Oddiel 8 – Autentifikácia webových lokalít

Tento oddiel je určený na to, aby sa zabezpečilo, že bude zaručená pravosť webovej lokality vo vzťahu k majiteľovi webovej lokality.

V článku 37 sa stanovujú požiadavky na kvalifikované certifikáty na autentifikáciu webových lokalít, ktoré sa môžu používať na zaručenie pravosti webovej lokality. Kvalifikovaný certifikát na autentifikáciu webových lokalít poskytne minimálny súbor dôveryhodných informácií o webovej lokalite a právnej existencii jej majiteľa.

3.3.4 KAPITOLA IV – DELEGOVANÉ AKTY

V článku 38 sa nachádzajú štandardné ustanovenia týkajúce sa výkonu delegácií v súlade s článkom 290 ZFEÚ (delegovaných aktov). Umožňuje to zákonodarcovi delegovať na Komisiu právomoc prijímať všeobecne záväzné nelegislatívne akty, ktorými sa dopĺňajú alebo menia určité nepodstatné prvky legislatívneho aktu.

3.3.5 KAPITOLA V – VYKONÁVACIE AKTY

Článok 39 obsahuje ustanovenie týkajúce sa postupu výboru potrebného na prenesenie vykonávacích právomocí na Komisiu, keď sú v súlade s článkom 291 ZFEÚ potrebné

jednotné podmienky vykonávania právne záväzných aktov Únie. Uplatňuje sa postup preskúmania.

3.3.6 KAPITOLA VI – ZÁVEREČNÉ USTANOVENIA

Článok 40 zaväzuje Komisiu, aby nariadenie vyhodnotila a podala správu o svojich zisteniach.

V článku 41 sa zrušuje smernica 1999/93/ES a stanovuje sa hladký prechod existujúcej infraštruktúry elektronických podpisov na nové požiadavky nariadenia.

V článku 42 sa stanovuje dátum nadobudnutia účinnosti tohto nariadenia.

4. VPLYV NA ROZPOČET

Osobitný vplyv návrhu na rozpočet sa týka úloh pridelených Európskej komisii, ako boli uvedené v legislatívnom finančnom výkaze pripojenom k tomuto návrhu.

Návrh nemá vplyv na operačné výdavky.

Legislatívny finančný výkaz pripojený k tomuto návrhu nariadenia pokrýva vplyv na rozpočet samotného nariadenia.

2012/0146 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

(Text s významom pre EHP)

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 predložení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[11],

po konzultácii s európskym dozorným úradníkom pre ochranu údajov[12],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) Vybudovanie dôvery v prostredí online je kľúčom k hospodárskemu rozvoju. V dôsledku nedostatku dôvery spotrebitelia, podniky a správne orgány váhajú s realizáciou elektronických transakcií a prijímaním nových služieb.

(2) Cieľom tohto nariadenia je posilniť dôveru pri elektronických transakciách na vnútornom trhu umožnením bezpečnej a plynulej realizácie elektronických interakcií medzi podnikmi, občanmi a verejnými orgánmi, čím sa zvýši efektivita verejných a súkromných služieb online, elektronického podnikania a elektronického obchodu v Únii.

(3) Smernica 1999/93/ES Európskeho parlamentu a Rady z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy[13] sa v podstate vzťahovala na elektronické podpisy bez toho, aby poskytla všeobecný cezhraničný a medziodvetvový rámec pre bezpečné, dôveryhodné a ľahko použiteľné elektronické transakcie. Týmto nariadením sa posilňuje a rozširuje *acquis* smernice.

---

11 Ú. v. EÚ C , , s. .

12 Ú. v. EÚ C , , s. .

13 Ú. v. ES L 13, 19.1.2000, s. 12.

(4) V Digitálnej agende pre Európu[14], ktorú vypracovala Komisia, sa identifikovala fragmentácia digitálneho trhu, nedostatočná interoperabilita a nárast počítačovej kriminality ako najväčšie prekážky pozitívneho kolobehu digitálneho hospodárstva. Komisia v správe o občianstve EÚ za rok 2010 ďalej zdôraznila potrebu vyriešiť hlavné problémy, ktoré bránia európskym občanom vo využívaní výhod digitálneho jednotného trhu a cezhraničných digitálnych služieb[15].

(5) Európska rada vyzvala Komisiu, aby vytvorila digitálny jednotný trh do roku 2015[16] s cieľom dosiahnuť rýchly pokrok v kľúčových oblastiach digitálneho hospodárstva a podporiť v plnej miere integrovaný digitálny jednotný trh[17] uľahčením cezhraničného používania služieb online, s osobitnou pozornosťou venovanou uľahčeniu bezpečnej elektronickej identifikácii a autentifikácii.

(6) Rada vyzvala Komisiu, aby prispela k digitálnemu jednotnému trhu vytvorením vhodných podmienok pre vzájomné uznávanie kľúčových prostriedkov naprieč hranicami, ako je elektronická identifikácia, elektronické dokumenty, elektronické podpisy a elektronické doručovacie služby, a pre interoperabilné služby elektronickej verejnej správy v celej Európskej únii[18].

(7) Európsky parlament zdôraznil význam bezpečnosti elektronických služieb, najmä elektronických podpisov a potreby vytvoriť infraštruktúru verejných kľúčov na celoeurópskej úrovni a vyzval Komisiu, aby vytvorila portály európskych orgánov potvrdzovania platnosti s cieľom zabezpečiť cezhraničnú interoperabilitu elektronických podpisov a zvýšiť bezpečnosť transakcií realizovaných prostredníctvom internetu[19].

(8) Smernica Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu[20] 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 ich vykonávanie na diaľku a elektronickými prostriedkami prostredníctvom príslušného miesta jednotného kontaktu a za súčinnosti príslušných orgánov. Mnohé služby online dostupné prostredníctvom miest jednotného kontaktu vyžadujú elektronickú identifikáciu, autentifikáciu a podpis.

(9) Vo väčšine prípadov poskytovatelia služieb z iného členského štátu nemôžu využívať svoju elektronickú identifikáciu na prístup k týmto službám, pretože národné systémy elektronickej identifikácie v ich krajine nie sú uznané a akceptované v iných členských štátoch. Táto elektronická bariéra bráni poskytovateľom služieb využívať výhody vnútorného trhu v plnej miere. Vzájomne uznávané a akceptované prostriedky elektronickej identifikácie uľahčia cezhraničné poskytovanie početných služieb na

---

14 KOM(2010) 245 v konečnom znení/2.

15 Správa o občianstve EÚ za rok 2010: Odstránenie prekážok vykonávania práv občanov EÚ, KOM(2010) 603 v konečnom znení, bod 2.2.2, strana 13.

16 4/2/2011: Dokument EUCO 2/1/11

17 23/10/2011: Dokument EUCO 52/1/11

18 Závery Rady k Európskemu akčnému plánu elektronickej verejnej správy na roky 2011 – 2015, 3093. zasadnutie Rady pre dopravu, telekomunikácie a energetiku, Brusel 27. mája 2011.

19 Uznesenie Európskeho parlamentu z 21.9.2010 o dobudovaní vnútorného trhu v oblasti elektronického obchodu, 21.9.10, P7_TA(2010)0320, a Uznesenie Európskeho parlamentu z 15.6.2010 o správe internetu: ďalšie kroky, P7_TA(2010)0208.

20 Ú. v. EÚ L 376, 27.12.2006, s. 36.

vnútornom trhu a umožnia podnikom expandovať do zahraničia bez toho, aby čelili mnohým prekážkam pri interakcii s orgánmi verejnej moci.

(10) Smernicou Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti[21] sa vytvára sieť vnútroštátnych orgánov zodpovedných za elektronické zdravotníctvo. S cieľom posilniť bezpečnosť a plynulosť cezhraničnej zdravotnej starostlivosti sa od tejto siete vyžaduje, aby vytvorila 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 a akceptovanie elektronickej identifikácie a autentifikácie je kľúčom k uskutočneniu 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) Jedným z cieľov tohto nariadenia je odstrániť existujúce prekážky cezhraničného využívania aspoň v prípade prostriedkov elektronickej identifikácie, ktoré sa v členských štátoch používajú na prístup k verejným službám. Cieľom tohto nariadenia nie je intervencia v 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.

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

(13) V nariadení je potrebné stanoviť určité podmienky, pokiaľ ide o to, ktoré prostriedky elektronickej identifikácie sa musia akceptovať, a ako by sa systémy mali oznamovať. To by členským štátom malo pomôcť pri budovaní potrebnej vzájomnej dôvery, pokiaľ ide o systémy elektronickej identifikácie, a pri vzájomnom uznávaní a akceptovaní prostriedkov elektronickej identifikácie v rámci nimi oznámených systémov. Zásada vzájomného uznávania a akceptovania by sa mala uplatňovať vtedy, keď oznamujúci členský štát splnil podmienky oznámenia a oznámenie bolo zverejnené v Úradnom vestníku Európskej únie. Prístup k týmto službám online a ich konečné poskytnutie žiadateľovi by však mali byť úzko spojené s právom na využívanie takýchto služieb na základe podmienok stanovených vo vnútroštátnych právnych predpisoch.

(14) Členské štáty by mali mať možnosť rozhodnúť o zapojení súkromného sektora do vydávania prostriedkov elektronickej identifikácie a umožniť, aby súkromný sektor využíval prostriedky elektronickej identifikácie v rámci oznámeného systému na účely identifikácie, keď sú potrebné na realizáciu služieb online alebo elektronických transakcií. Možnosť používať takéto prostriedky elektronickej identifikácie by

[21] Ú. v. EÚ L 88, 4.4.2011, s. 45.

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 občanom a podnikom by uľahčila prístup k ich službám online naprieč hranicami. Pre uľahčenie cezhraničného využívania takýchto prostriedkov elektronickej identifikácie súkromným sektorom by možnosť autentifikácie poskytovaná členskými štátmi mala byť dostupná pre závislé strany bez rozdielov medzi verejným a súkromným sektorom.

(15) Cezhraničné používanie prostriedkov elektronickej identifikácie v rámci oznámeného systému vyžaduje, aby členské štáty spolupracovali na zabezpečení technickej interoperability. Na základe tejto potreby sa vylučujú akékoľvek konkrétne vnútroštátne technické pravidlá, ktoré by vyžadovali, aby napríklad nenárodné závislé strany získali konkrétny hardvér alebo softvér na overenie a potvrdenie platnosti oznámenej elektronickej identifikácie. Na druhej strane sú nevyhnutné technické požiadavky na používateľov, vyplývajúce z inherentných špecifikácií ktoréhokoľvek používaného tokenu (napríklad čipových kariet).

(16) Spolupráca členských štátov by mala slúžiť technickej interoperabilite oznámených systémov elektronickej identifikácie s cieľom podporiť vysokú mieru dôvery a bezpečnosti, primeranú stupňu rizika. Výmena informácií a zdieľanie najlepšej praxe medzi členskými štátmi s cieľom zabezpečiť vzájomné uznávanie by mali pomáhať takejto spolupráci.

(17) Týmto nariadením by sa ďalej mal stanoviť všeobecný právny rámec pre používanie dôveryhodných elektronických služieb. Nemala by sa ním však stanoviť všeobecná povinnosť používať tieto služby. Konkrétne by sa nemalo vzťahovať na poskytovanie služieb na základe dobrovoľných dohôd v rámci súkromného práva. Nemalo by sa vzťahovať ani na aspekty súvisiace s uzavretím a platnosťou zmlúv alebo iných právnych povinností, pri ktorých existujú požiadavky na formu predpísanú vnútroštátnymi zákonmi alebo právnymi predpismi Únie.

(18) S cieľom prispieť k všeobecnému cezhraničnému používaniu dôveryhodných elektronických služieb by malo byť možné používať ich ako dôkazy v súdnom konaní vo všetkých členských štátoch.

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

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

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

(22) S cieľom posilniť dôveru ľudí vo vnútorný trh a podporiť používanie dôveryhodných služieb a produktov by sa mali zaviesť pojmy kvalifikované dôveryhodné služby a kvalifikovaný poskytovateľ dôveryhodných služieb so zámerom uviesť požiadavky a povinnosti na zabezpečenie vysokej úrovne bezpečnosti akýchkoľvek používaných alebo poskytovaných kvalifikovaných dôveryhodných služieb a produktov.

(23) V súlade s povinnosťami v rámci Dohovoru OSN o právach osôb so zdravotným postihnutím, ktorý nadobudol platnosť v EÚ, by osoby s postihnutím mali mať možnosť využívať dôveryhodné služby a produkty pre koncových používateľov používané pri poskytovaní týchto služieb na rovnakých základoch ako iní spotrebitelia.

(24) Poskytovateľ dôveryhodných služieb je kontrolór osobných údajov, a preto musí plniť povinnosti stanovené v smernici Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov[22]. Najmä zber údajov by sa mal čo najviac minimalizovať so zreteľom na účel poskytovanej služby.

(25) Orgány dohľadu by mali spolupracovať a vymieňať si informácie s orgánmi na ochranu údajov s cieľom zabezpečiť, aby poskytovatelia služieb riadne vykonávali právne predpisy o ochrane údajov. Výmena informácií by sa mala vzťahovať najmä na bezpečnostné incidenty a narušenia bezpečnosti osobných údajov.

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

(27) Ustanovenia o používaní pseudonymov v certifikátoch by nemali členským štátom brániť v tom, aby vyžadovali identifikáciu osôb podľa zákonov Únie alebo vnútroštátnych zákonov.

(28) Všetky členské štáty by mali dodržiavať spoločné základné požiadavky na dohľad 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 najlepšej praxi v tejto oblasti.

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

(30) Aby Komisia a členské štáty mohli posúdiť efektívnosť mechanizmu oznamovania narušenia zavedeného týmto nariadením, malo by sa vyžadovať, aby orgány dohľadu Komisii a Európskej agentúre pre bezpečnosť sietí a informácií (ENISA) poskytovali súhrnné informácie.

(31) Aby Komisia a členské štáty mohli posúdiť vplyv tohto nariadenia, malo by sa vyžadovať, aby orgány dohľadu poskytovali štatistiku kvalifikovaných dôveryhodných služieb a ich používania.

(32) 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. Je 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.

---

22 Ú. v. EÚ L 281, 23.11.1995, s. 31.

(33) S cieľom zabezpečiť trvalú udržateľnosť a trvácnosť kvalifikovaných dôveryhodných služieb a posilniť dôveru používateľov v kontinuitu kvalifikovaných dôveryhodných služieb by orgány dohľadu mali zabezpečiť, aby sa údaje kvalifikovaných poskytovateľov dôveryhodných služieb primerane dlho uchovávali a zostávali dostupné, aj keď kvalifikovaný poskytovateľ dôveryhodných služieb zanikne.

(34) 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.

(35) Zodpovednosťou poskytovateľov dôveryhodných služieb je splniť požiadavky týkajúce sa poskytovania dôveryhodných služieb, ktoré sú stanovené v tomto nariadení, a to predovšetkým kvalifikovaných dôveryhodných služieb. Zodpovednosťou orgánov dohľadu je dohliadať na to, ako poskytovatelia dôveryhodných služieb tieto požiadavky spĺňajú.

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

(37) Zoznamy dôveryhodných informácií sú prvky, ktoré sú podstatné pre vybudovanie dôvery medzi trhovými subjektmi, pretože potvrdzujú kvalifikovaný štatút poskytovateľa služieb v čase dohľadu, na druhej strane však nie sú nevyhnutným predpokladom na dosiahnutie kvalifikovaného štatútu a poskytovanie kvalifikovaných dôveryhodných služieb, ktoré vyplýva z dodržiavania požiadaviek tohto nariadenia.

(38) Keď už raz kvalifikovaná dôveryhodná služba bola predmetom oznámenia, príslušný subjekt verejného sektora ju nemôže odmietnuť pri plnení administratívneho postupu alebo formality preto, že sa nenachádza v zoznamoch dôveryhodných informácií vytvorených členskými štátmi. Na tento účel sa orgánom verejného sektora rozumie akýkoľvek verejný orgán alebo iný subjekt poverený poskytovaním služieb elektronickej verejnej správy, ako je podávanie daňových priznaní online, žiadosť o vydanie rodného listu, účasť na postupoch elektronického verejného obstarávania atď.

(39) Vysoká úroveň bezpečnosti je potrebná na zabezpečenie vzájomného uznávania elektronických podpisov v osobitných prípadoch, ako v kontexte rozhodnutia 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[23], mali by sa však akceptovať aj elektronické podpisy s nižšou zárukou bezpečnosti.

(40) Signatár by mal mať možnosť zveriť zariadenia na vytvorenie kvalifikovaného elektronického podpisu do starostlivosti tretej strany za predpokladu, že sa zavedú

[23] Ú. v. EÚ L 274, 20.10.2009, s. 36.

vhodné mechanizmy a postupy, ktorými sa zabezpečí, že signatár bude mať výlučnú kontrolu nad používaním svojich údajov na vytvorenie elektronického podpisu a že pri používaní zariadenia budú splnené požiadavky na kvalifikovaný podpis.

(41) Na zabezpečenie právnej istoty v súvislosti s platnosťou podpisu je nevyhnutné určiť zložky kvalifikovaného elektronického podpisu, ktoré musí posúdiť závislá strana vykonávajúca potvrdenie platnosti. Navyše vymedzenie požiadaviek na kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí môžu poskytovať kvalifikovanú službu potvrdzovania platnosti závislým stranám, ktoré nechcú, alebo nemôžu samy vykonávať potvrdzovanie platnosti kvalifikovaných elektronických podpisov, by malo stimulovať súkromný alebo verejný sektor, aby investoval do takýchto služieb. Obidva prvky by mali všetkým stranám na úrovni Únie uľahčiť a zjednodušiť potvrdzovanie platnosti kvalifikovaných elektronických podpisov.

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

(43) Elektronické pečate slúžia ako dôkaz, že elektronický dokument vydala právnická osoba a zabezpečujú istotu, pokiaľ ide o pôvod a neporušenosť dokumentu.

(44) Týmto nariadením by sa malo zaručiť dlhodobé uchovávanie informácií, t. j. právna platnosť elektronického podpisu a elektronických pečatí počas rozšírených období, pričom by sa malo zaručiť, aby sa mohli overiť bez ohľadu na budúce technologické zmeny.

(45) S cieľom posilniť cezhraničné využívanie elektronických dokumentov by sa v tomto nariadení mal stanoviť právny účinok elektronických dokumentov, ktoré by sa mali považovať za rovnocenné s papierovými dokumentmi v závislosti od posúdenia rizík a za predpokladu, že je zabezpečená pravosť a neporušenosť dokumentov. Pre ďalší rozvoj cezhraničných elektronických transakcií na vnútornom trhu je dôležité aj to, aby sa originálne elektronické dokumenty alebo certifikované kópie vydané danými príslušnými orgánmi v členskom štáte v súlade s jeho vnútroštátnymi právnymi predpismi akceptovali ako také aj v iných členských štátoch. Toto nariadenie by nemalo mať vplyv na právo členských štátov určiť, čo tvorí originál alebo kópiu na vnútroštátnej úrovni, ale zabezpečuje sa ním, aby sa mohli používať ako také aj cezhranične.

(46) 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 nevyhnutné zabezpečiť, aby podporovali aspoň niektoré formáty zdokonalených elektronických pečatí.

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

(48) Keď sa umožní autentifikácia webových lokalít a osoby, ktorá ich vlastní, sťaží sa falšovanie webových lokalít, a tak sa zníži množstvo podvodov.

(49) S cieľom doplniť určité podrobné technické aspekty tohto nariadenia pružným a rýchlym spôsobom by sa na Komisiu mala preniesť právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie, pokiaľ ide o interoperabilitu elektronickej identifikácie; bezpečnostné opatrenia, ktoré sa vyžadujú od poskytovateľov dôveryhodných služieb; uznávané nezávislé subjekty zodpovedné za vykonávanie auditov poskytovateľov služieb; zoznamy dôveryhodných informácií; požiadavky týkajúce sa úrovní bezpečnosti elektronických podpisov; požiadavky na kvalifikované certifikáty pre elektronické podpisy, ich overenie a uchovávanie; subjekty zodpovedné za certifikáciu zariadení na vytvorenie kvalifikovaných elektronických podpisov; a požiadavky týkajúce sa úrovní bezpečnosti elektronických pečatí a kvalifikovaných certifikátov pre elektronické pečate; interoperabilitu doručovacích služieb. Je osobitne dôležité, aby Komisia počas svojich prípravných prác uskutočnila náležité konzultácie, a to aj na expertnej úrovni.

(50) Pri príprave a vypracovávaní delegovaných aktov by mala Komisia zabezpečiť súčasné, včasné a vhodné postúpenie príslušných dokumentov Európskemu parlamentu a Rade.

(51) S cieľom zabezpečiť podmienky vykonávania tohto nariadenia by sa Komisii mali udeliť vykonávacie právomoci, najmä pokiaľ ide o špecifikovanie referenčných čísel noriem, ktorých použitie by dávalo predpoklad súladu s určitými požiadavkami stanovenými v tomto nariadení alebo vymedzenými v delegovaných aktoch. Tieto právomoci by sa mali vykonávať v súlade s nariadením 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[24].

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

(53) S cieľom zabezpečiť právnu istotu pre prevádzkovateľov na trhu, ktorí už používajú kvalifikované certifikáty vydané v súlade so smernicou 1999/93/ES, je nevyhnutné stanoviť dostatočné prechodné obdobie. Zároveň je nevyhnutné, aby sa Komisii poskytli prostriedky na prijímanie vykonávacích aktov a delegovaných aktov pred uvedeným dátumom.

(54) 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, Únia môže prijať opatrenia v súlade so zásadou subsidiarity, ako je uvedené v článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality stanovenou v uvedenom článku toto nariadenie neprekračuje rámec potrebný na dosiahnutie tohto cieľa, najmä pokiaľ ide o úlohu Komisie ako koordinátorky vnútroštátnych činností,

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

[24] Ú. v. EÚ L 55, 28.2.2011, s. 13.

Článok 1

Predmet úpravy

1. V tomto nariadení sa stanovujú pravidlá pre elektronickú identifikáciu a dôveryhodné elektronické služby pre elektronické transakcie s cieľom zabezpečiť správne fungovanie vnútorného trhu.

2. V tomto nariadení sa stanovujú podmienky, za ktorých členské štáty uznávajú a akceptujú prostriedky elektronickej identifikácie fyzických a právnických osôb, ktoré patria do oznámeného systému elektronickej identifikácie iného členského štátu.

3. V tomto nariadení sa vytvára právny rámec pre elektronické podpisy, elektronické pečate, elektronické časové pečiatky, elektronické dokumenty, elektronické doručovacie služby a autentifikáciu webových lokalít.

4. Týmto nariadením sa zabezpečuje, aby dôveryhodné služby a produkty, ktoré sú v súlade s týmto nariadením, mali povolenie na voľný obeh na vnútornom trhu.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa vzťahuje na elektronickú identifikáciu poskytovanú členskými štátmi a poskytovateľmi dôveryhodných služieb usadenými v Únii alebo poskytovanú v ich mene alebo pod ich dohľadom.

2. Toto nariadenie sa nevzťahuje na poskytovanie dôveryhodných elektronických služieb na základe dobrovoľných dohôd v rámci súkromného práva.

3. Toto nariadenia sa nevzťahuje na aspekty súvisiace s uzavretím a platnosťou zmlúv alebo iných právnych povinností, pri ktorých existujú požiadavky na formu predpísanú vnútroštátnymi zákonmi alebo právnymi predpismi Únie.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

(1) „elektronická identifikácia“ je proces používania osobných identifikačných údajov v elektronickej forme jednoznačne reprezentujúcich fyzickú alebo právnickú osobu;

(2) „prostriedok elektronickej identifikácie“ je fyzická jednotka obsahujúca údaje, ako sa uvádza v bode 1 tohto článku, ktorá sa používa na prístup k službám online, ako sa uvádza v článku 5;

(3) „systém elektronickej identifikácie“ je systém elektronickej identifikácie, v rámci ktorého sa osobám uvedeným v bode 1 tohto článku vydávajú prostriedky elektronickej identifikácie.

(4) „autentifikácia“ je elektronický proces, ktorý umožňuje overiť elektronickú identifikáciu fyzickej alebo právnickej osoby; alebo pôvod a neporušenosť elektronických údajov;

(5) „signatár“ je fyzická osoba, ktorá vytvára elektronický podpis;

(6) „elektronický podpis“ sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným elektronickým údajom a ktoré signatár používa na podpisovanie;

(7) „zdokonalený elektronický podpis“ je elektronický podpis, ktorý spĺňa nasledujúce požiadavky:

(a) je jedinečne spojený so signatárom;

(b) je schopný identifikovať signatára;

(c) je vytvorený pomocou údajov na vytvorenie elektronického podpisu, ktoré môže signatár s vysokou mierou istoty používať s výlučnou kontrolou; a

(d) je prepojený s údajmi, na ktoré sa vzťahuje, takým spôsobom, že každú dodatočnú zmenu údajov možno hneď zistiť;

(8) „kvalifikovaný elektronický podpis“ je zdokonalený elektronický podpis vytvorený pomocou zariadenia na vytvorenie kvalifikovaného elektronického podpisu, ktorý je založený na kvalifikovanom certifikáte pre elektronické podpisy;

(9) „údaje na vytvorenie elektronického podpisu“ sú jedinečné údaje, ktoré používa signatár na vytvorenie elektronického podpisu;

(10) „certifikát“ je elektronické osvedčenie, ktoré spája údaje na overenie elektronického podpisu alebo pečate fyzickej alebo právnickej osoby s certifikátom a potvrdzuje tieto údaje o príslušnej osobe;

(11) „kvalifikovaný certifikát elektronického podpisu“ je osvedčenie, ktoré sa používa na potvrdenie elektronických podpisov, vydáva ho kvalifikovaný poskytovateľ dôveryhodných služieb a toto osvedčenie musí spĺňať požiadavky stanovené v prílohe I;

(12) „dôveryhodná služba“ je akákoľvek elektronická služba spočívajúca vo vytváraní, potvrdzovaní, overovaní, spracovávaní a uchovávaní elektronických podpisov, elektronických pečatí, elektronických časových pečiatok, elektronických dokumentov, elektronických doručovacích služieb, autentifikácie webových lokalít a elektronických certifikátov vrátane certifikátov elektronických podpisov a elektronických pečatí;

(13) „kvalifikovaná dôveryhodná služba“ je dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky stanovené v tomto nariadení;

(14) „poskytovateľ dôveryhodných služieb“ je fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb;

(15) „kvalifikovaný poskytovateľ dôveryhodných služieb“ je poskytovateľ dôveryhodných služieb, ktorý spĺňa požiadavky stanovené v tomto nariadení;

(16) „produkt“ je hardvér alebo softvér alebo jeho príslušné zložky určené na použitie v rámci poskytovania dôveryhodných služieb;

(17) „zariadenie na vytvorenie elektronického podpisu“ je nakonfigurovaný softvér alebo hardvér používaný na vytvorenie elektronického podpisu;

(18) „zariadenie na vytvorenie kvalifikovaného elektronického podpisu“ je zariadenie na vytvorenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II;

(19) „autor pečate“ je právnická osoba, ktorá vytvára elektronickú pečať;

(20) „elektronická pečať“ sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným elektronickým údajom s cieľom zabezpečiť pôvod a neporušenosť priradených údajov;

(21) „zdokonalená elektronická pečať“ je elektronická pečať, ktorá spĺňa nasledujúce požiadavky:

(a) je jedinečne spojená s autorom pečate;

(b) je schopná identifikovať autora pečate;

(c) je vytvorená pomocou údajov na vytvorenie elektronickej pečate, ktoré môže autor pečate s vysokou mierou istoty používať na vytvorenie elektronickej pečate s výlučnou kontrolou; a

(d) je prepojený s údajmi, na ktoré sa vzťahuje, takým spôsobom, že každú dodatočnú zmenu údajov možno hneď zistiť;

(22) „kvalifikovaná elektronická pečať“ je zdokonalená elektronická pečať vytvorená pomocou zariadenia na vytvorenie kvalifikovanej elektronickej pečate, ktorá je založená na kvalifikovanom certifikáte elektronickej pečate;

(23) „údaje na vytvorenie elektronickej pečate“ sú jedinečné údaje, ktoré používa autor elektronickej pečate na vytvorenie elektronickej pečate;

(24) „kvalifikovaný certifikát elektronickej pečate“ je osvedčenie, ktoré sa používa na potvrdenie elektronickej pečate, vydáva ho kvalifikovaný poskytovateľ dôveryhodných služieb a toto osvedčenie musí spĺňať požiadavky stanovené v prílohe III;

(25) „elektronická časová pečiatka“ sú údaje v elektronickej forme, ktoré viažu iné elektronické údaje s konkrétnym časom, čím tvoria dôkaz o existencii týchto údajov v danom čase;

(26) „kvalifikovaná elektronická časová pečiatka“ je elektronická časová pečiatka, ktorá spĺňa požiadavky stanovené v článku 33;

(27) „elektronický dokument“ je dokument v akomkoľvek elektronickom formáte;

(28) „elektronická doručovacia služba“ je služba, ktorá umožňuje elektronické posielanie údajov a poskytuje dôkazy týkajúce sa spracovania odoslaných údajov vrátane dôkazu o odoslaní alebo prijatí údajov a ktorá chráni odosielané údaje pred rizikom straty, krádeže, poškodenia alebo akýchkoľvek neoprávnených úprav;

(29) „kvalifikovaná elektronická doručovacia služba“ je elektronická doručovacia služba, ktorá spĺňa požiadavky stanovené v článku 36;

(30) „kvalifikovaný certifikát autentifikácie webovej lokality“ je osvedčenie, ktoré umožňuje autentifikáciu webovej lokality a spája túto webovú lokalitu s osobou, ktorej bol certifikát vystavený; vydáva ho kvalifikovaný poskytovateľ dôveryhodných služieb a musí spĺňať požiadavky stanovené v prílohe IV;

(31) „overovacie údaje“ sú údaje, ktoré sa používajú na overenie elektronického podpisu alebo elektronickej pečiatky.

Článok 4

Zásada vnútorného trhu

1. Neexistuje žiadne obmedzenie poskytovania dôveryhodných služieb na území členského štátu poskytovateľom dôveryhodných služieb usadeným v inom členskom štáte z dôvodov, ktoré patria do oblastí, na ktoré sa vzťahuje toto nariadenie.

2. Na vnútornom trhu sa povoľuje voľný obeh produktov, ktoré sú v súlade s týmto nariadením.

KAPITOLA II

ELEKTRONICKÁ IDENTIFIKÁCIA

Článok 5

Vzájomné uznávanie a akceptovanie

Keď sa podľa vnútroštátnych právnych predpisov alebo administratívnej praxe vyžaduje elektronická identifikácia využívajúca prostriedok elektronickej identifikácie a autentifikáciu, akýkoľvek prostriedok elektronickej identifikácie vydaný v inom členskom štáte patriaci do systému začleneného zoznamu uverejneného Komisiou v súlade s postupom uvedeným v článku 7, sa uznáva a akceptuje na účely prístupu k tejto službe.

Článok 6

Podmienky oznamovania systémov elektronickej identifikácie

1. Systémy elektronickej identifikácie sú oprávnené na oznámenie podľa článku 7, ak sú splnené všetky tieto podmienky:

(a) prostriedky elektronickej identifikácie sú vydané členským štátom, ktorý oznamuje daný systém, v jeho mene alebo pod dohľadom tohto členského štátu;

(b) prostriedky elektronickej identifikácie sa môžu použiť na prístup aspoň k verejným službám, ktoré vyžadujú elektronickú identifikáciu v oznamujúcom členskom štáte;

(c) oznamujúci členský štát zabezpečuje, aby boli osobné identifikačné údaje jednoznačne priradené fyzickej alebo právnickej osobe, ako sa uvádza v článku 3 bode 1;

(d) oznamujúci členský štát zabezpečuje dostupnosť možnosti autentifikácie online kedykoľvek a bezplatne, aby si každá závislá strana mohla overiť osobné identifikačné údaje, ktoré prijala v elektronickej forme. Členské štáty nesmú uložiť žiadne konkrétne technické požiadavky závislým stranám usadeným mimo ich územia, ktoré chcú vykonať takúto autentifikáciu. Keď sa naruší alebo čiastočne kompromituje buď oznámený systém identifikácie, alebo možnosť autentifikácie, členské štáty bezodkladne pozastavia alebo odvolajú oznámený systém identifikácie alebo možnosť autentifikácie alebo ich príslušné kompromitované časti a informujú o tom ostatné členské štáty a Komisiu v súlade s článkom 7;

(e) oznamujúci členský štát nesie zodpovednosť za:

– i) jednoznačné priradenie osobných identifikačných údajov uvedených v písmene c), a

– ii) možnosť autentifikácie uvedenú v písmene d).

2. Ustanovenie v písmene e) odseku 1 nemá vplyv na zodpovednosť strán transakcie, v ktorej sa používajú prostriedky elektronickej identifikácie patriace do oznámeného systému.

Článok 7

Oznámenia

1. Členské štáty, ktoré oznamujú systémy elektronickej identifikácie, odovzdajú Komisii tieto informácie a bez zbytočného meškania všetky ich následné zmeny:

(a) opis oznámeného systému elektronickej identifikácie;

(b) orgány zodpovedné za oznámený systém elektronickej identifikácie;

(c) informácie o tom, kto spravuje registráciu jednoznačných osobných identifikátorov;

(d) opis možnosti autentifikácie;

(e) podmienky pozastavenia alebo zrušenia buď oznámeného systému identifikácie, alebo možnosti autentifikácie, alebo ich príslušných kompromitovaných častí.

2. Šesť mesiacov po nadobudnutí účinnosti nariadenia Komisia v *Úradnom vestníku Európskej únie* zverejní zoznam systémov elektronickej identifikácie oznámených podľa odseku 1 a základné informácie o nich.

3. Ak Komisia dostane oznámenie po uplynutí lehoty uvedenej v odseku 2, zoznam do troch mesiacov zmení a doplní.

4. Komisia môže prostredníctvom vykonávacích aktov definovať okolnosti, formáty a postupy oznámenia uvedené v odsekoch 1 a 3. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 8

Koordinácia

1. Členské štáty spolupracujú na zabezpečení interoperability prostriedkov elektronickej identifikácie patriacich do oznámeného systému a na zvýšení ich bezpečnosti.

2. Komisia prostredníctvom vykonávacích aktov stanoví potrebné spôsoby s cieľom uľahčiť spoluprácu medzi členskými štátmi uvedenú v odseku 1, so zámerom podporiť vysokú úroveň dôvery a bezpečnosti primeranú stupňu rizika. Tieto vykonávacie akty sa budú týkať najmä výmeny informácií, skúseností a osvedčených postupov v oblasti systémov elektronickej identifikácie, partnerského preskúmania oznámených systémov elektronickej identifikácie a preskúmania príslušného vývoja v sektore elektronickej identifikácie príslušnými orgánmi členských štátov. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o uľahčenie cezhraničnej interoperability prostriedkov elektronickej identifikácie stanovením minimálnych technických požiadaviek.

KAPITOLA III

DÔVERYHODNÉ SLUŽBY

Oddiel 1

Všeobecné ustanovenia

Článok 9

Zodpovednosť

1. Poskytovateľ dôveryhodných služieb je zodpovedný za každú priamu škodu spôsobenú akejkoľvek fyzickej alebo právnickej osobe pre nedodržanie povinností stanovených v článku 15 ods. 1, pokiaľ poskytovateľ dôveryhodných služieb nedokáže, že nekonal nedbanlivo.

2. Kvalifikovaný poskytovateľ dôveryhodných služieb je zodpovedný za každú priamu škodu spôsobenú akejkoľvek fyzickej alebo právnickej osobe pre nedodržanie požiadaviek stanovených v tomto nariadení, najmä v článku 19, pokiaľ kvalifikovaný poskytovateľ dôveryhodných služieb nedokáže, že nekonal nedbanlivo.

Článok 10

Poskytovatelia dôveryhodných služieb z tretích krajín

1. Kvalifikované dôveryhodné služby a kvalifikované certifikáty poskytnuté kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými v tretej krajine sa akceptujú ako kvalifikované dôveryhodné služby a kvalifikované certifikáty poskytnuté kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými na území Únie, ak sú kvalifikované dôveryhodné služby alebo kvalifikované certifikáty pochádzajúce z tretej krajiny uznané v rámci dohody medzi Úniou a tretími krajinami alebo medzinárodnými organizáciami v súlade s článkom 218 ZFEÚ.

2. S odkazom na odsek 1 takéto podmienky zabezpečia, že poskytovatelia dôveryhodných služieb v tretích krajinách alebo medzinárodných organizáciách splnia požiadavky vzťahujúce sa na kvalifikované dôveryhodné služby a kvalifikované certifikáty poskytované kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými na území Únie, najmä so zreteľom na ochranu osobných údajov, bezpečnosť a dohľad.

Článok 11

Spracovanie a ochrana údajov

1. Poskytovatelia dôveryhodných služieb a orgány dohľadu zabezpečia pri spracovaní osobných údajov spravodlivé a zákonné postupy v súlade so smernicou 95/46/ES.

2. Poskytovatelia dôveryhodných služieb spracúvajú osobné údaje v súlade so smernicou 95/46/ES. Takéto spracovanie sa prísne obmedzuje na minimálne údaje potrebné na vydanie a uchovávanie certifikátu alebo na poskytovanie dôveryhodných služieb.

3. Poskytovatelia dôveryhodných služieb zaručia dôvernosť a neporušenosť údajov týkajúcich sa osoby, ktorej poskytujú dôveryhodnú službu.

4. Bez toho, aby bol dotknutý právny účinok vzťahujúci sa na pseudonymy podľa vnútroštátneho práva, členské štáty nesmú brániť poskytovateľom dôveryhodných služieb, aby v certifikátoch elektronických podpisov uvádzali pseudonym namiesto mena signatára.

Článok 12

Dostupnosť pre osoby so zdravotným postihnutím

Vždy, keď je možné, dôveryhodné služby poskytované a produkty pre koncových užívateľov používané pri poskytovaní týchto služieb sa sprístupňujú osobám so zdravotným postihnutím.

Oddiel 2

Dohľad

Článok 13

Orgán dohľadu

1. Členské štáty určia vhodný subjekt usadený na ich území, alebo, po vzájomnej dohode, v inom členskom štáte, pod dohľadom určujúceho členského štátu. Orgány dohľadu dostanú všetky dozorné a vyšetrovacie právomoci potrebné na vykonávanie ich úloh.

2. Orgán dohľadu je zodpovedný za vykonávanie týchto úloh:

(a) monitorovanie poskytovateľov dôveryhodných služieb usadených na území určujúceho členského štátu s cieľom zabezpečiť, aby dodržiavali požiadavky stanovené v článku 15;

(b) vykonávanie dohľadu nad kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými na území určujúceho členského štátu a nad kvalifikovanými dôveryhodnými službami, ktoré poskytujú, s cieľom zabezpečiť, aby oni i kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňali uplatniteľné požiadavky stanovené v tomto nariadení;

(c) zabezpečovanie, aby sa relevantné informácie a údaje uvedené v písmene g) článku 19 ods. 2 a zaznamenané kvalifikovanými poskytovateľmi dôveryhodných služieb primerane dlho uchovávali a aby zostávali dostupné aj po ukončení činnosti kvalifikovaného poskytovateľa dôveryhodných služieb v záujme zaručenia kontinuity služby.

3. Každý orgán dohľadu Komisii a členským štátom predloží výročnú správu o činnostiach dohľadu za posledný kalendárny rok do konca prvého štvrťroka nasledujúceho roka. Táto správa obsahuje aspoň:

(a) informácie o jeho činnostiach dohľadu;

(b) zhrnutie oznámení o narušení prijatých od poskytovateľov dôveryhodných služieb v súlade s článkom 15 ods. 2;

(c) štatistiku trhu a používania kvalifikovaných dôveryhodných služieb vrátane informácií o samotných kvalifikovaných poskytovateľoch dôveryhodných služieb, o kvalifikovaných dôveryhodných službách, ktoré poskytujú, o produktoch, ktoré používajú, a všeobecného opisu ich zákazníkov.

4. Členské štáty oznámia Komisii a ostatným členským štátom názvy a adresy svojich určených orgánov dohľadu.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o definovanie postupov vzťahujúcich sa na úlohy uvedené v odseku 2.

6. Komisia môže prostredníctvom vykonávacích aktov definovať okolnosti, formáty a postupy správy uvedenej v odseku 3. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 14

Vzájomná pomoc

1. Orgány dohľadu si s cieľom vymeniť si osvedčené postupy v čo najkratšom čase navzájom poskytujú relevantné informácie a vzájomnú pomoc, aby sa činnosti mohli vykonávať konzistentne. Vzájomná pomoc zahŕňa najmä žiadosti o informácie a opatrenia dohľadu, ako sú žiadosti o vykonanie inšpekcií súvisiacich s bezpečnostnými auditmi, ako sa uvádza v článkoch 15, 16 a 17.

2. Ak je dozornému orgánu adresovaná žiadosť o pomoc, nemôže jej odmietnuť vyhovieť, s výnimkou toho, keď:

(a) nie je nekompetentný na vybavenie tejto žiadosti; alebo

(b) vyhovenie žiadosti by nebolo zlučiteľné s týmto nariadením.

3. Ak je to vhodné, orgány dohľadu môžu vykonávať spoločné vyšetrovania, do ktorých sa zapoja zamestnanci orgánov dohľadu z iných členských štátov.

Orgán dohľadu členského štátu, v ktorom sa má vyšetrovanie uskutočniť, v súlade s vlastnými vnútroštátnymi právnymi predpismi môže vyšetrovacie úlohy preniesť na zamestnancov orgánu dohľadu, ktorému pomáha. Takéto právomoci sa môžu vykonávať iba pod usmernením a v prítomnosti zamestnancov hostiteľského orgánu dohľadu. Zamestnanci orgánu dohľadu, ktorému hostiteľský orgán dohľadu pomáha, podliehajú vnútroštátnym právnym predpisom hostiteľského orgánu dohľadu. Hostiteľský orgán dohľadu preberá zodpovednosť za konanie zamestnancov orgánu dohľadu, ktorému pomáha.

4. Komisia môže prostredníctvom vykonávacích aktov špecifikovať formáty a postupy vzájomnej pomoci stanovenej v tomto článku. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 15

Bezpečnostné požiadavky vzťahujúce sa na poskytovateľov dôveryhodných služieb

1. Poskytovatelia dôveryhodných služieb vrátane kvalifikovaných poskytovateľov dôveryhodných služieb usadení na území Únie vykonávajú vhodné technické a organizačné opatrenia v rámci riadenia rizík ohrozujúcich bezpečnosť dôveryhodných služieb, ktoré poskytujú. So zreteľom na najnovšie technológie tieto opatrenia musia zabezpečiť úroveň bezpečnosti primeranú stupňu rizika. Vykonajú najmä opatrenia prevencie a minimalizácie vplyvu bezpečnostných incidentov a zainteresovaným stranám oznámia nepriaznivé účinky prípadných incidentov.

Bez toho, aby bol dotknutý článok 16 ods. 1, každý poskytovateľ dôveryhodných služieb môže orgánu dohľadu predložiť správu z bezpečnostného auditu, ktorý vykonal uznávaný nezávislý subjekt, s cieľom potvrdiť vykonanie primeraných bezpečnostných opatrení.

2. Poskytovatelia dôveryhodných služieb do 24 hodín príslušnému orgánu dohľadu, príslušnému vnútroštátnemu orgánu pre bezpečnosť informácií a ďalším relevantným tretím stranám, ako sú orgány na ochranu údajov, oznámia každé narušenie bezpečnosti alebo stratu neporušenosti s významným vplyvom na poskytovanú dôveryhodnú službu a osobné údaje uchovávané v rámci nej.

Ak je to vhodné, a najmä keď sa narušenie bezpečnosti alebo strata neporušenosti týka dvoch alebo viacerých členských štátov, dotknutý orgán dohľadu o veci informuje orgány dohľadu v iných členských štátoch a Európsku agentúru pre bezpečnosť sietí a informácií (ENISA).

Dotknutý orgán dohľadu môže informovať aj verejnosť, alebo požiadať o to poskytovateľa dôveryhodných služieb, ak zistí, že zverejnenie narušenia je vo verejnom záujme.

3. Orgán dohľadu agentúre ENISA a Komisii každoročne poskytuje zhrnutie oznámení o narušení, ktoré prijal od poskytovateľov dôveryhodných služieb.

4. Na účely vykonávania odsekov 1 a 2 má príslušný orgán dohľadu právomoc vydávať záväzné pokyny pre poskytovateľov dôveryhodných služieb.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o ďalšie špecifikovanie opatrení uvedených v odseku 1.

6. Komisia môže prostredníctvom vykonávacích aktov definovať okolnosti, formáty a postupy vrátane lehôt, uplatniteľné na účel odsekov 1 až 3. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 16

Dohľad nad kvalifikovanými poskytovateľmi dôveryhodných služieb

1. Kvalifikovaní poskytovatelia dôveryhodných služieb sa raz ročne podrobia auditu uznávaného nezávislého subjektu, aby sa potvrdilo, že oni sami, ako aj kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v tomto nariadení, a orgánu dohľadu predložia výslednú správu z bezpečnostného auditu.

2. Bez toho, aby bol dotknutý odsek 1, orgán dohľadu môže kedykoľvek vykonať audit kvalifikovaných poskytovateľov dôveryhodných služieb s cieľom potvrdiť, že oni sami, ako aj kvalifikované dôveryhodné služby, ktoré poskytujú, stále spĺňajú podmienky stanovené v tomto nariadení, buď z vlastnej iniciatívy, alebo v reakcii na žiadosť Komisie. Orgán dohľadu orgánom na ochranu údajov oznámi výsledky svojich auditov v prípade, že sa zdá, že došlo k porušeniu pravidiel ochrany osobných údajov.

3. Orgán dohľadu má právomoc vydať kvalifikovaným poskytovateľom služieb záväzné pokyny na nápravu akéhokoľvek nedodržania požiadaviek uvedeného v správe z bezpečnostného auditu.

4. S odkazom na odsek 3, ak kvalifikovaný poskytovateľ dôveryhodných služieb nenapraví takéto nedodržanie v lehote, ktorú mu určí orgán dohľadu, stráca svoj kvalifikovaný štatút a orgán dohľadu mu oznámi, že sa jeho štatút v zoznamoch dôveryhodných informácií uvedených v článku 18 primerane zmení.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o špecifikovanie podmienok uznania nezávislého subjektu vykonávajúceho audit uvedený v odseku 1 tohto článku, článku 15 ods. 1 a článku 17 ods. 1.

6. Komisia môže prostredníctvom vykonávacích aktov definovať okolnosti, postupy a formáty uplatniteľné na účel odsekov 1, 2 a 4. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 17

Začatie kvalifikovanej dôveryhodnej služby

1. Kvalifikovaní poskytovatelia dôveryhodných služieb orgánu dohľadu oznámia svoj úmysel začať poskytovať kvalifikovanú dôveryhodnú službu a predložia mu správu z bezpečnostného auditu, ktorý vykonal uznávaný nezávislý subjekt, ako sa stanovuje v článku 16 ods. 1. Kvalifikovaní poskytovatelia dôveryhodných služieb môžu začať poskytovať kvalifikovanú dôveryhodnú službu potom, keď orgánu dohľadu predložili oznámenie a správu z bezpečnostného auditu.

2. Po predložení príslušných dokumentov orgánu dohľadu podľa odseku 1 sa kvalifikovaní poskytovatelia služieb zaradia do zoznamov dôveryhodných informácií uvedených v článku 18, v ktorých sa zaznamená predloženie oznámenia.

3. Orgán dohľadu overí súlad kvalifikovaného poskytovateľa dôveryhodnej služby a kvalifikovaných dôveryhodných služieb, ktoré ponúka, s požiadavkami nariadenia.

Orgán dohľadu vyznačí kvalifikovaný štatút kvalifikovaných poskytovateľov služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú, v zoznamoch dôveryhodných informácií po pozitívnom uzavretí overenia, najneskôr do jedného mesiaca po vykonaní oznámenia v súlade s odsekom 1.

Ak sa overovanie neukončí do jedného mesiaca, orgán dohľadu o tom informuje kvalifikovaného poskytovateľa dôveryhodných služieb a oznámi mu dôvody meškania a lehotu, v ktorej sa overovanie ukončí.

4. Kvalifikovanú dôveryhodnú službu, ktorá bola predmetom oznámenia uvedeného v odseku 1, príslušný subjekt verejného sektora nemôže odmietnuť pri plnení administratívneho postupu alebo formality preto, že sa nenachádza v zoznamoch uvedených v odseku 3.

5. Komisia môže prostredníctvom vykonávacích aktov definovať okolnosti, formáty a postupy na účel odsekov 1, 2 a 3. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 18

Zoznamy dôveryhodných informácií

1. Každý členský štát vytvorí, vedie a zverejňuje zoznamy dôveryhodných informácií s informáciami týkajúcimi sa kvalifikovaných poskytovateľov dôveryhodných služieb, pre ktorých je kompetentný, spolu s informáciami týkajúcimi sa kvalifikovaných dôveryhodných služieb, ktoré poskytujú.

2. Členské štáty bezpečne vytvoria, vedú a zverejnia elektronicky podpísané alebo zapečatené zoznamy dôveryhodných informácií stanovené v odseku 1 formou vhodnou na automatizované spracovanie.

3. Členské štáty Komisii bez zbytočného meškania oznámia informácie o subjekte zodpovednom za vytvorenie, vedenie a zverejnenie vnútroštátnych zoznamov dôveryhodných informácií, ako aj údaje o tom, kde sa tieto zoznamy zverejnia, o certifikáte použitom na podpísanie alebo zapečatenie zoznamov dôveryhodných informácií a o všetkých ich zmenách.

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

5. Komisia sa splnomocňuje prijímať delegované akty v súlade s článkom 38 týkajúce sa vymedzenia informácií uvedených v odseku 1.

6. Komisia môže prostredníctvom vykonávacích aktov definovať technické špecifikácie a formáty zoznamov dôveryhodných informácií na účely odsekov 1 až 4. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 19

Požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb

1. Pri vydávaní kvalifikovaného certifikátu kvalifikovaný poskytovateľ dôveryhodnej služby vhodnými prostriedkami a v súlade s vnútroštátnymi právnymi predpismi overuje identitu a ak je to vhodné, akékoľvek konkrétne atribúty fyzickej alebo právnickej osoby, ktorej vystavuje kvalifikovaný certifikát.

Kvalifikovaný poskytovateľ služieb alebo poverená tretia strana konajúca pod dohľadom kvalifikovaného poskytovateľa služieb tieto informácie overuje:

(a) podľa fyzického vzhľadu fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, alebo

(b) na diaľku, pomocou prostriedkov elektronickej identifikácie patriacich do oznámeného systému vydaného v súlade s písmenom a).

2. Kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí poskytujú kvalifikované dôveryhodné služby:

(a) zamestnávajú zamestnancov, ktorí disponujú potrebnými odbornými znalosťami, skúsenosťami a kvalifikáciami, uplatňujú administratívne a riadiace postupy zodpovedajúce európskym alebo medzinárodným normám a získali primerané odborné vzdelanie v oblasti pravidiel bezpečnosti a ochrany osobných údajov;

(b) nesú riziko zodpovednosti za škodu udržiavaním dostatočných finančných zdrojov alebo prostredníctvom vhodného poistenia zodpovednosti za škodu;

(c) pred uzavretím zmluvného vzťahu informujú každú osobu, ktorá chce využívať kvalifikovanú dôveryhodnú službu, o presných podmienkach využívania tejto služby;

(d) používajú dôveryhodné systémy a produkty chránené proti pozmeneniu a zaručujú technickú bezpečnosť a spoľahlivosť procesu, ktorý podporujú;

(e) používajú dôveryhodné systémy na ukladanie im poskytnutých údajov v overiteľnej forme tak, aby:

– boli verejne dostupné a vyhľadateľné iba po získaní súhlasu osoby, ktorej boli údaje vystavené,

– zápisy a zmeny mohli robiť len oprávnené osoby,

– bolo možné skontrolovať pravosť informácií;

(f) vykonávajú opatrenia proti falšovaniu a krádeži údajov;

(g) zaznamenávajú počas vhodného obdobia všetky relevantné informácie týkajúce sa údajov vydaných a prijatých kvalifikovaným poskytovateľom dôveryhodných služieb, najmä na účel poskytnutia dôkazov v súdnom konaní. Toto zaznamenávanie sa môže realizovať elektronicky;

(h) majú pripravený aktuálny plán ukončenia s cieľom zabezpečiť kontinuitu služby v súlade s podmienkami vydanými orgánom dohľadu podľa článku 13 ods. 2 písmena c).

(i) zabezpečujú zákonné spracovanie osobných údajov v súlade s článkom 11.

3. Kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty, vo svojej databáze certifikátov zaregistrujú zrušenie certifikátu do desiatich minút od nadobudnutia účinnosti takéhoto zrušenia.

4. So zreteľom na odsek 3, kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty, každej závislej strane poskytnú informácie o platnosti alebo zrušení štatútu kvalifikovaných certifikátov, ktoré sami vydali. Tieto informácie sa poskytujú kedykoľvek, prinajmenšom na základe certifikátov, automatickým spôsobom, ktorý je spoľahlivý, bezplatný a efektívny.

5. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre dôveryhodné systémy a produkty. Súlad s požiadavkami stanovenými v odseku 19 sa predpokladá vtedy, ak dôveryhodné systémy a produkty spĺňajú uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Oddiel 3

Elektronický podpis

Článok 20

Právne účinky a akceptovanie elektronických podpisov

1. Právny účinok elektronického podpisu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne na základe toho, že má elektronickú formu.

2. Kvalifikovaný elektronický podpis má právny účinok ekvivalentný s podpisom písaným rukou.

3. Kvalifikované elektronické podpisy sa uznávajú a akceptujú vo všetkých členských štátoch.

4. Ak sa vyžaduje elektronický podpis s úrovňou zaručenia bezpečnosti nižšou ako kvalifikovaný elektronický podpis, najmä ak takýto elektronický podpis vyžaduje členský štát na prístup k službe online, ktorú ponúka subjekt verejného sektora, na základe primeraného posúdenia rizík, ktoré hrozia pri takejto službe, uznávajú a akceptujú sa všetky elektronické podpisy zodpovedajúce aspoň rovnakej úrovni zaručenia bezpečnosti.

5. Členské štáty na cezhraničný prístup k službe online, ktorú ponúka subjekt verejného sektora, nevyžadujú elektronický podpis vyššej úrovne zaručenia bezpečnosti ako kvalifikovaný elektronický podpis.

6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o definovanie rôznych úrovní bezpečnosti elektronického podpisu uvedených v odseku 4.

7. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre úrovne bezpečnosti elektronického podpisu. Súlad s úrovňou bezpečnosti definovanou v delegovanom akte prijatom podľa odseku 6 sa predpokladá vtedy, ak elektronický podpis spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 21

Kvalifikované certifikáty elektronických podpisov

1. Kvalifikované certifikáty elektronických podpisov musia spĺňať požiadavky stanovené v prílohe I.

2. Kvalifikované certifikáty elektronických podpisov nepodliehajú žiadnym povinným požiadavkám prekračujúcim požiadavky stanovené v prílohe I.

3. Ak sa po počiatočnej aktivácii zruší kvalifikovaný certifikát elektronických podpisov, stráca svoju platnosť a jeho štatút sa za žiadnych okolností obnovením jeho platnosti nezmení na pôvodný.

4. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o ďalšie špecifikovanie požiadaviek stanovených v prílohe I.

5. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre kvalifikované certifikáty elektronického podpisu. Súlad s požiadavkami stanovenými v prílohe I sa predpokladá vtedy, ak kvalifikovaný certifikát elektronických podpisov spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 22

Požiadavky na zariadenia na vytvorenie kvalifikovaných elektronických podpisov

1. Zariadenia na vytvorenie kvalifikovaného elektronického podpisu musia spĺňať požiadavky stanovené v prílohe II.

2. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre zariadenia na vytvorenie kvalifikovaných elektronických podpisov. Súlad s požiadavkami stanovenými v prílohe II sa predpokladá vtedy, ak zariadenie na vytvorenie kvalifikovaného elektronického podpisu spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 23

Certifikácia zariadení na vytvorenie kvalifikovaného elektronického podpisu

1. Zariadenia na vytvorenie kvalifikovaného elektronického podpisu môžu certifikovať vhodné verejné alebo súkromné subjekty určené členskými štátmi za predpokladu, že sa podrobili procesu vyhodnotenia bezpečnosti, ktorý sa vykonal v súlade s jednou z noriem pre bezpečnostné posúdenie produktov informačných technológií, uvedených na zozname, ktorý vytvorí Komisia pomocou vykonávacích aktov. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

2. Členské štáty oznámia Komisii a ostatným členským štátom názov a adresu verejného alebo súkromného subjektu, ktorý určili tak, ako sa uvádza v odseku 1.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o stanovenie osobitných kritérií, ktoré musia splniť určené subjekty uvedené v odseku 1.

Článok 24

Zverejňovanie zoznamu certifikovaných zariadení na vytvorenie kvalifikovaného elektronického podpisu

1. Členské štáty Komisii bez zbytočného meškania oznámia informácie o zariadeniach na vytvorenie kvalifikovaného elektronického podpisu, ktoré certifikovali subjekty uvedené v článku 23. Komisii ďalej bez zbytočného meškania oznámia informácie o zariadeniach na vytvorenie elektronického podpisu, ktoré už nie sú certifikované.

2. Komisia na základe získaných informácií vytvára, zverejňuje a vedie zoznam certifikovaných zariadení na vytvorenie kvalifikovaného elektronického podpisu.

3. Komisia môže prostredníctvom vykonávacích aktov definovať okolnosti, formáty a postupy uplatniteľné na účely odseku 1. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 25

Požiadavky na overenie kvalifikovaných elektronických podpisov

1. Kvalifikovaný elektronický podpis sa považuje za platný vtedy, ak s vysokou mierou istoty možno preukázať, že v čase podpísania:

(a) certifikát, ktorý potvrdzuje podpis, je kvalifikovaným certifikátom elektronického podpisu, ktorý je v súlade s ustanoveniami stanovenými v prílohe I;

(b) požadovaný kvalifikovaný certifikát je pravý a platný;

(c) údaje na overenie podpisu zodpovedajú údajom poskytnutým závislej strane;

(d) súbor údajov jednoznačne reprezentujúcich signatára je správne poskytnutý závislej strane;

(e) použitie akéhokoľvek pseudonymu sa jasne uvádza, ak sa používa pseudonym;

(f) elektronický podpis bol vytvorený zariadením na vytvorenie kvalifikovaného elektronického podpisu;

(g) neporušenosť podpísaných údajov nebola kompromitovaná;

(h) sú splnené požiadavky stanovené v článku 3 bode 7;

(i) systém použitý na overenie podpisu poskytuje závislej strane správny výsledok procesu overenia a umožňuje závislej strane odhaliť akékoľvek problémy súvisiace s bezpečnosťou.

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o ďalšie špecifikovanie požiadaviek stanovených v odseku 1.

3. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre overenie kvalifikovaných elektronických podpisov. Súlad s požiadavkami stanovenými v odseku 1 sa predpokladá vtedy, ak overenie kvalifikovaných elektronických podpisov spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 26

Kvalifikovaná služba overovania kvalifikovaných elektronických podpisov

1. Kvalifikovanú službu overovania kvalifikovaných elektronických podpisov poskytuje kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý:

(a) poskytuje overovanie v súlade s článkom 25 ods. 1, a

(b) závislým stranám umožňuje dostávať výsledok overovacieho procesu automatizovaným spôsobom, ktorý je spoľahlivý, účinný a ktorý obsahuje zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať poskytovateľa kvalifikovanej služby overovania.

2. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre kvalifikovanú službu overovania uvedenú v odseku 1. Súlad s požiadavkami stanovenými v písmene b) odseku 1 sa predpokladá vtedy, ak služba overovania kvalifikovaných elektronických podpisov spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 27

Uchovávanie kvalifikovaných elektronických podpisov

1. Službu uchovávania kvalifikovaných elektronických podpisov poskytuje kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý používa postupy a technológie, ktoré umožňujú rozšíriť dôveryhodnosť údajov na overenie kvalifikovaného elektronického podpisu aj po uplynutí technologickej platnosti.

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o ďalšie špecifikovanie požiadaviek stanovených v odseku 1.

3. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre uchovávanie kvalifikovaných elektronických podpisov. Súlad s požiadavkami stanovenými v odseku 1 sa predpokladá vtedy, ak podmienky uchovávania kvalifikovaných elektronických podpisov zodpovedajú uvedeným normám. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Oddiel 4

Elektronické pečate

Článok 28

Právne účinky elektronických pečatí

1. Právny účinok elektronickej pečate a jej prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne na základe toho, že má elektronickú formu.

2. Na kvalifikovanú elektronickú pečať sa vzťahuje právna domnienka zaručujúca pôvod a neporušenosť údajov, s ktorými je spojená.

3. Kvalifikovaná elektronická pečať sa uznáva a akceptuje vo všetkých členských štátoch.

4. Ak sa vyžaduje elektronická pečať s úrovňou zaručenia bezpečnosti nižšou ako kvalifikovaná elektronická pečať, najmä ak takúto elektronickú pečať vyžaduje členský štát na prístup k službe online, ktorú ponúka subjekt verejného sektora, na základe primeraného posúdenia rizík, ktoré hrozia pri takejto službe, akceptujú sa všetky elektronické pečate zodpovedajúce aspoň rovnakej úrovni zaručenia bezpečnosti.

5. Členské štáty na prístup k službe online, ktorú ponúka subjekt verejného sektora, nevyžadujú elektronickú pečať vyššej úrovne zaručenia bezpečnosti ako kvalifikované elektronické pečate.

6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o definovanie rôznych úrovní zaručenia bezpečnosti elektronických pečatí uvedených v odseku 4.

7. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre úrovne zaručenia bezpečnosti elektronických pečatí. Súlad s úrovňou zaručenia bezpečnosti definovanou v delegovanom akte prijatom podľa odseku 6 sa predpokladá vtedy, ak elektronická pečať spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 29

Požiadavky na kvalifikované certifikáty elektronickej pečate

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

2. Kvalifikované certifikáty elektronickej pečate nepodliehajú žiadnym povinným požiadavkám prekračujúcim požiadavky stanovené v prílohe III.

3. Ak sa po počiatočnej aktivácii zruší kvalifikovaný certifikát elektronickej pečate, stráca svoju platnosť a jeho štatút sa za žiadnych okolností obnovením jeho platnosti nezmení na pôvodný.

4. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o ďalšie špecifikovanie požiadaviek stanovených v prílohe III.

5. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre kvalifikované certifikáty elektronickej pečate. Súlad s požiadavkami stanovenými v prílohe III sa predpokladá vtedy, ak kvalifikovaný certifikát elektronickej pečate spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Článok 30

Zariadenia na vytvorenie kvalifikovaných elektronických pečatí

1. Článok 22 sa primerane uplatňuje na požiadavky na zariadenia na vytvorenie kvalifikovaných elektronických pečatí.

2. Článok 23 sa primerane uplatňuje na certifikáciu zariadení na vytvorenie kvalifikovaných elektronických pečatí.

3. Článok 24 sa primerane uplatňuje na zverejňovanie zoznamu certifikovaných zariadení na vytvorenie kvalifikovaných elektronických pečatí.

Článok 31

Potvrdzovanie platnosti a uchovávanie kvalifikovaných elektronických pečatí

Články 25, 26 a 27 sa uplatňujú primerane na potvrdzovanie platnosti a uchovávanie kvalifikovaných elektronických pečatí.

Oddiel 5

Elektronická časová pečiatka

Článok 32

Právny účinok elektronických časových pečiatok

1. Právny účinok elektronickej časovej pečiatky a jej prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne na základe toho, že má elektronickú formu.

2. Na kvalifikovanú elektronickú časovú pečiatku sa vzťahuje právna domnienka zaručujúca správnosť času, ktorý uvádza, a neporušenosť údajov, s ktorými je spojená.

3. Kvalifikovaná elektronická časová pečiatka sa uznáva a akceptuje vo všetkých členských štátoch.

Článok 33

Požiadavky na kvalifikované elektronické časové pečiatky.

1. Kvalifikovaná elektronická časová pečiatka musí spĺňať tieto požiadavky:

(a) musí byť presne spojená s koordinovaným svetovým časom (UTC) takým spôsobom, aby sa zamedzila akákoľvek možnosť nezistiteľnej zmeny údajov;

(b) musí byť založená na presnom zdroji času;

(c) musí byť vydaná kvalifikovaným poskytovateľom dôveryhodných služieb;

(d) musí byť podpísaná zdokonaleným elektronickým podpisom alebo zdokonalenou elektronickou pečaťou kvalifikovaného poskytovateľa dôveryhodných služieb, alebo ekvivalentným spôsobom.

2. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre presné prepojenie času s údajmi a s presným zdrojom času. Súlad s požiadavkami stanovenými v odseku 1 sa predpokladá vtedy, ak presné prepojenie času s údajmi a s presným zdrojom času spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Oddiel 6

Elektronické dokumenty

Článok 34

Právne účinky a akceptovanie elektronických dokumentov

1. Elektronický dokument sa považuje za ekvivalentný s papierovým dokumentom a je prípustný ako dôkaz v súdnom konaní so zreteľom na jeho úroveň zaručenia pravosti a neporušenosti.

2. Na dokument s kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou osoby, ktorá je oprávnená príslušný dokument vydať, sa vzťahuje právna domnienka jeho pravosti a neporušenosti za predpokladu, že dokument neobsahuje dynamické prvky, ktoré môžu dokument automaticky zmeniť.

3. Keď sa na poskytnutie služby online, ktorú ponúka subjekt verejného sektora, vyžaduje originálny dokument alebo certifikovaná kópia, prinajmenšom elektronické dokumenty vydané osobami, ktoré majú právomoc vydávať príslušné dokumenty a ktoré sa považujú za originály alebo certifikované kópie v súlade s vnútroštátnymi právnymi predpismi členského štátu pôvodu, sa akceptujú v iných členských štátoch bez dodatočných požiadaviek.

4. Komisia môže prostredníctvom vykonávacích aktov definovať formáty elektronických podpisov a pečatí, ktoré sa akceptujú vždy, keď členský štát vyžaduje dokument s podpisom alebo pečaťou na poskytovanie služby online, ktorú ponúka subjekt verejného sektora, ako sa uvádza v odseku 2. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Oddiel 7

Kvalifikovaná elektronická doručovacia služba

Článok 35

Právny účinok elektronickej doručovacej služby

1. Údaje odoslané alebo prijaté prostredníctvom elektronickej doručovacej služby sú prípustné ako dôkaz v súdnom konaní so zreteľom na neporušenosť údajov a istotu dátumu a času odoslania alebo prijatia údajov určeným adresátom.

2. Na údaje odoslané alebo prijaté prostredníctvom kvalifikovanej elektronickej doručovacej služby sa vzťahuje právna domnienka neporušenosti údajov a presnosti dátumu a času odoslania alebo prijatia údajov.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o špecifikovanie mechanizmov odosielania a prijímania údajov prostredníctvom elektronických doručovacích služieb, ktoré sa používajú so zámerom posilniť interoperabilitu medzi elektronickými doručovacími službami.

Článok 36

Požiadavky na kvalifikované elektronické doručovacie služby

1. Kvalifikované elektronické doručovacie služby musia spĺňať tieto požiadavky:

(a) musí ich poskytovať jeden alebo viacerí kvalifikovaní poskytovatelia dôveryhodných služieb;

(b) musia umožňovať jednoznačnú identifikáciu odosielateľa a ak je to vhodné, adresáta;

(c) proces odosielania alebo prijímania údajov musí byť zabezpečený zdokonaleným elektronickým podpisom alebo zdokonalenou elektronickou pečaťou kvalifikovaného poskytovateľa dôveryhodných služieb takým spôsobom, aby sa zamedzila akákoľvek možnosť nezistiteľnej zmeny údajov;

(d) akákoľvek zmena údajov potrebná na účel odoslania alebo prijatia údajov sa musí jasne oznámiť odosielateľovi a adresátovi údajov;

(e) dátum odoslania, prijatia a akejkoľvek zmeny údajov sa musí oznámiť kvalifikovanou elektronickou časovou pečiatkou;

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

2. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre procesy odosielania a prijímania údajov. Súlad s požiadavkami stanovenými v odseku 1 sa predpokladá vtedy, ak proces odosielania a prijímania údajov spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

Oddiel 8

Autentifikácia webových lokalít

Článok 37

Požiadavky na kvalifikované certifikáty autentifikácie webových lokalít

1. Kvalifikované certifikáty autentifikácie webových lokalít musia spĺňať požiadavky stanovené v prílohe IV.

2. Kvalifikované certifikáty autentifikácie webových lokalít sa uznávajú a akceptujú vo všetkých členských štátoch.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38, pokiaľ ide o ďalšie špecifikovanie požiadaviek stanovených v prílohe IV.

4. Komisia môže prostredníctvom vykonávacích aktov vytvoriť referenčné čísla noriem pre kvalifikované certifikáty autentifikácie webových lokalít. Súlad s požiadavkami stanovenými v prílohe IV sa predpokladá vtedy, ak kvalifikovaný certifikát autentifikácie webových lokalít spĺňa uvedené normy. Tieto vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. Komisia uverejňuje tieto akty v *Úradnom vestníku Európskej únie*.

KAPITOLA IV

DELEGOVANÉ AKTY

Článok 38

Vykonávanie delegovania právomoci

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

2. Právomoc prijímať delegované akty uvedené v článkoch 8 ods. 3, 13 ods. 5, 15 ods. 5, 16 ods. 5, 18 ods. 5, 20 ods. 6, 21 ods. 4, 23 ods. 3, 25 ods. 2, 27 ods. 2, 28 ods. 6, 29 ods. 4, 30 ods. 2, 31, 35 ods. 3 a 37 ods. 3 sa prenáša na Komisiu na dobu neurčitú od nadobudnutia účinnosti tohto nariadenia.

3. Delegovanie právomocí uvedených v článkoch 8 ods. 3, 13 ods. 5, 15 ods. 5, 16 ods. 5, 18 ods. 5, 20 ods. 6, 21 ods. 4, 23 ods. 3, 25 ods. 2, 27 ods. 2, 28 ods. 6, 29 ods. 4, 30 ods. 2, 31, 35 ods. 3 a 37 ods. 3 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci uvedenej v tomto rozhodnutí. 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 hneď po prijatí delegovaného aktu túto skutočnosť oznámi súčasne Európskemu parlamentu a Rade.

5. Delegovaný akt prijatý podľa článkov 8 ods. 3, 13 ods. 5, 15 ods. 5, 16 ods. 5, 18 ods. 5, 20 ods. 6, 21 ods. 4, 23 ods. 3, 25 ods. 2, 27 ods. 2, 28 ods. 6, 29 ods. 4, 30 ods. 2, 31, 35 ods. 3 a 37 ods. 3 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.

KAPITOLA V

VYKONÁVACIE AKTY

Článok 39

Postup výboru

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

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

KAPITOLA VI

ZÁVEREČNÉ USTANOVENIA

Článok 40

Správa

Komisia Európskemu parlamentu a Rade podáva správy o uplatňovaní tohto nariadenia. Prvú správu predloží najneskôr do štyroch rokov po nadobudnutí účinnosti tohto nariadenia. Následné správy bude potom predkladať každé štyri roky.

Článok 41

Zrušenie

1. Smernica 1999/93/ES sa zrušuje.

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

3. Bezpečné zariadenia na vytvorenie podpisu, ktorých súlad sa stanovil v súlade s článkom 3 ods. 4 smernice 1999/93/ES, sa podľa tohto nariadenia považujú za zariadenia na vytvorenie kvalifikovaného podpisu.

4. Kvalifikované certifikáty vydané podľa smernice 1999/93/ES sa považujú za kvalifikované certifikáty elektronických podpisov podľa tohto nariadenia do vypršania ich platnosti, nie však dlhšie než päť rokov po nadobudnutí účinnosti tohto nariadenia.

Článok 42

Nadobudnutie účinnosti

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

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

V Bruseli

Za Európsky parlament
predseda

Za Radu
predseda

PRÍLOHA I

Požiadavky na kvalifikované certifikáty elektronických podpisov

Kvalifikované certifikáty elektronických podpisov obsahujú:

(a) označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný certifikát elektronického podpisu;

(b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, prinajmenšom vrátane členského štátu, v ktorom je poskytovateľ usadený, a

- v prípade právnickej osoby: názov a registračné číslo tak, ako sa uvádza v úradných záznamoch,
- v prípade fyzickej osoby: meno osoby;

(c) súbor údajov jednoznačne reprezentujúcich signatára, ktorému sa certifikát vydáva, prinajmenšom vrátane mena signatára alebo jeho pseudonymu, ktorý musí byť označený ako pseudonym;

(d) údaje na potvrdenie platnosti elektronického podpisu, ktoré zodpovedajú údajom na vytvorenie elektronického podpisu;

(e) údaje o začiatku a konci 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 bezplatne dostupný certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať, uvedené v písmene g);

(i) lokalitu služieb súvisiacich so stavom platnosti certifikátov, ktoré sa môžu využiť na bezplatné zistenie stavu platnosti kvalifikovaného certifikátu;

(j) ak sa údaje na vytvorenie elektronického podpisu súvisiace s údajmi na overenie elektronického podpisu nachádzajú v zariadení na vytvorenie kvalifikovaného elektronického podpisu, primerané uvedenie tejto skutočnosti, prinajmenšom vo forme vhodnej na automatizované spracovanie.

PRÍLOHA II

Požiadavky na zariadenia na vytvorenie kvalifikovaných podpisov

1. Zariadenia na vytvorenie kvalifikovaných elektronických podpisov musia vhodnými technickými a procedurálnymi prostriedkami zabezpečovať prinajmenšom, aby:

(a) bola zaručená dôvernosť údajov na vytvorenie elektronického podpisu použitých na vytvorenie elektronického podpisu;

(b) údaje na vytvorenie elektronického podpisu použité na vytvorenie elektronického podpisu sa mohli objaviť iba raz;

(c) údaje na vytvorenie elektronického podpisu použité na vytvorenie elektronického podpisu nebolo možné s primeraným uistením odvodiť a elektronický podpis bol chránený proti falšovaniu pomocou technológií dostupných v súčasnosti;

(d) oprávnený signatár mohol údaje na vytvorenie elektronického podpisu použité na vytvorenie elektronického podpisu spoľahlivo chrániť pred použitím inými osobami.

2. Zariadenia na vytvorenie kvalifikovaného elektronického podpisu nesmú meniť údaje, ktoré sa majú podpísať, ani brániť, aby sa tieto údaje ukázali signatárovi pred podpísaním.

3. Vytvorenie alebo spravovanie údajov na vytvorenie elektronického podpisu v mene signatára uskutočňuje kvalifikovaný poskytovateľ dôveryhodných služieb.

4. Kvalifikovaní poskytovatelia dôveryhodných služieb spravujúci údaje na vytvorenie elektronického podpisu v mene signatára môžu údaje na vytvorenie elektronického podpisu duplikovať na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:

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

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

PRÍLOHA III

Požiadavky na kvalifikované certifikáty elektronických pečatí

Kvalifikované certifikáty elektronických pečatí obsahujú:

(a) označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný certifikát elektronického podpisu;

(b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, prinajmenšom vrátane členského štátu, v ktorom je poskytovateľ usadený, a

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

– v prípade fyzickej osoby: meno osoby;

(c) súbor údajov jednoznačne reprezentujúcich právnickú osobu, ktorej sa certifikát vydáva, prinajmenšom vrátane názvu a registračného čísla tak, ako sa uvádza v úradných záznamoch;

(d) údaje na overenie elektronickej pečate, ktoré zodpovedajú údajom na vytvorenie elektronickej pečate;

(e) údaje o začiatku a konci 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 bezplatne dostupný certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať, uvedené v písmene g);

(i) lokalitu služieb súvisiacich so stavom platnosti certifikátov, ktoré sa môžu využiť na bezplatné zistenie stavu platnosti kvalifikovaného certifikátu;

(j) ak sa údaje na vytvorenie elektronickej pečate súvisiace s údajmi na overenie elektronickej pečate nachádzajú v zariadení na vytvorenie kvalifikovanej elektronickej pečate, primerané uvedenie tejto skutočnosti, prinajmenšom vo forme vhodnej na automatizované spracovanie.

PRÍLOHA IV

Požiadavky na kvalifikované certifikáty autentifikácie webových lokalít

Kvalifikované certifikáty autentifikácie webových lokalít obsahujú:

(a) označenie, prinajmenšom vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný certifikát elektronického podpisu;

(b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, prinajmenšom vrátane členského štátu, v ktorom je poskytovateľ usadený, a

- v prípade právnickej osoby: názov a registračné číslo tak, ako sa uvádza v úradných záznamoch,
- v prípade fyzickej osoby: meno osoby;

(c) súbor údajov jednoznačne reprezentujúcich právnickú osobu, ktorej sa certifikát vydáva, prinajmenšom vrátane názvu a registračného čísla tak, ako sa uvádza v úradných záznamoch;

(d) prvky adresy prinajmenšom vrátane mesta a členského štátu právnickej osoby, ktorej sa certifikát vystavuje tak, ako sa uvádza v úradných záznamoch;

(e) názvy domén prevádzkovaných právnickou osobou, ktorej sa certifikát vystavuje;

(f) údaje o začiatku a konci 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 bezplatne dostupný certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať, uvedené v písmene h);

(j) lokalitu služieb súvisiacich so stavom platnosti certifikátov, ktoré sa môžu využiť na bezplatné zistenie stavu platnosti kvalifikovaného certifikátu;

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

Tento finančný výkaz obsahuje požiadavky z hľadiska administratívnych výdavkov na vykonanie navrhovaného nariadenia o *elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu*.

Po legislatívnom postupe a diskusii o prijatí navrhovaného nariadenia Európskym parlamentom a Radou bude Komisia vyžadovať dvanásť jednotiek ekvivalentu plného pracovného času na prípravu súvisiacich delegovaných a vykonávacích aktov s cieľom zabezpečiť dostupnosť organizačných a technických noriem na spracovanie informácií oznámených členskými štátmi, najmä na uchovávanie informácií týkajúcich sa dôveryhodných zoznamov, na zabezpečenie informovanosti zainteresovaných strán – najmä občanov a MSP – o výhodách využívania elektronickej identifikácie, autentifikácie, podpisov a súvisiacich dôveryhodných služieb (eIAS) a na rozprúdenie diskusií s tretími krajinami s cieľom dosiahnuť interoperabilitu služieb eIAS na celosvetovej úrovni.

1.1. Názov návrhu/iniciatívy

Návrh nariadenia Komisie o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

1.2. Príslušné oblasti politiky v rámci ABM/ABB[25]

09 INFORMAČNÁ SPOLOČNOSŤ

1.3. Druh návrhu/iniciatívy

☐ Návrh/iniciatíva sa týka **novej akcie**

☐ Návrh/iniciatíva sa týka **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[26]

☐ Návrh/iniciatíva sa týka **predĺženia trvania existujúcej akcie**

☑ Návrh/iniciatíva sa týka **akcie presmerovanej na novú akciu**

1.4. Ciele

1.4.1. Viacročné strategické ciele Komisie, ktoré sú predmetom návrhu/iniciatívy

Všeobecné ciele návrhu sú cieľmi všeobecných politík EÚ, v ktorých oblasti sa návrh nachádza, ako je stratégia Európa 2020. Jej cieľom je zabezpečiť, aby sa Európa „zmenila na inteligentné, trvalo udržateľné a inkluzívne hospodárstvo dosahujúce vysokú úroveň zamestnanosti, produktivity a sociálne súdržnosti.“

25 ABM: riadenie podľa činností – ABB: zostavovanie rozpočtu podľa činností.

26 Podľa článku 49 ods. 6 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

1.4.2. Konkrétne ciele a príslušné činnosti v rámci ABM/ABB

Posilniť dôveru v celoeurópske elektronické transakcie a zabezpečiť cezhraničné právne uznávanie elektronickej identifikácie, autentifikácie, podpisov a súvisiacich dôveryhodných služieb, ako aj vysokú úroveň ochrany údajov a posilnenia postavenia používateľov na vnútornom trhu (pozri Digitálnu agendu pre Európu, kľúčové opatrenia 3 a 16).

Príslušné činnosti v rámci ABM/ABB

09 02 - Regulačný rámec pre Digitálnu agendu pre Európu

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na príjemcov/cieľové skupiny.

Vytvoriť pre služby eIAS jasné regulačné prostredie, ktoré posilní pohodlie, dôveru a istotu používateľov v digitálnom svete.

1.4.4. Ukazovatele výsledkov a vplyvu

Uveďte ukazovatele, pomocou ktorých je možné sledovať uskutočňovanie návrhu/iniciatívy.

1. Existencia dodávateľov služieb eIAS, ktorí vyvíjajú činnosti vo viacerých členských štátoch EÚ:

2. Stupeň interoperability zariadení (napríklad čítačky čipových kariet) naprieč sektormi, krajinami;

3. Využívanie služieb eIAS všetkými kategóriami obyvateľstva;

4. Rozsah, v akom služby eIAS využívajú koncoví používatelia na vnútroštátne a medzinárodné (cezhraničné) transakcie;

5. Stupeň harmonizácie právnych predpisov o službách eIAS naprieč členskými štátmi;

6. Systémy elektronickej identifikácie oznámené Komisii;

7. Služby prístupné pomocou prostriedkov oznámenej elektronickej identifikácie vo verejnom sektore (elektronická verejná správa, elektronické zdravotníctvo, elektronická justícia, elektronické verejné obstarávanie);

8. Služby prístupné pomocou prostriedkov oznámenej elektronickej identifikácie v súkromnom sektore (internetbanking, elektronický obchod, elektronické hazardné hry, prihlasovanie sa na webové lokality, služby bezpečnejšieho internetu).

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte

Rozdielne národné implementácie smernice o elektronickom podpise v dôsledku rozdielnych výkladov členských štátov v súvislosti so súčasnou smernicou vedú k problémom s cezhraničnou interoperabilitou a v dôsledku toho aj k segmentovanému prostrediu v EÚ a narušeniu vnútorného trhu. Túto situáciu sprevádza nedostatok istoty a dôvery v elektronické systémy, ktorý bráni európskym občanom využívať v digitálnom svete rovnaké služby ako vo fyzickom svete.

1.5.2. Prínos zapojenia do Európskej únie

Akcia na úrovni EÚ by v porovnaní s akciou na úrovni členských štátov priniesla jasné výhody. Skúsenosti skutočne ukázali, že opatrenia na vnútroštátnej úrovni sú nielen nedostatočné na umožnenie cezhraničných elektronických transakcií, ale dokonca naopak vytvorili bariéry pre interoperabilitu elektronických podpisov v celej EÚ a v súčasnosti majú rovnaký účinok aj na elektronickú identifikáciu, elektronickú autentifikáciu a súvisiace dôveryhodné služby.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Tento návrh vychádza zo skúseností so smernicou o elektronickom podpise a problémov, ktoré sa objavujú pre fragmentovanú transpozíciu a implementáciu tejto smernice a ktoré je bránia v dosiahnutí stanovených cieľov.

1.5.4. Zlučiteľnosť a možná synergia s inými finančnými nástrojmi

Odkazy na smernicu o elektronickom podpise sa nachádzajú vo viacerých iniciatívach EÚ vytvorených s cieľom odstrániť problémy s interoperabilitou a cezhraničným uznávaním a akceptovaním v súvislosti s určitými druhmi elektronických interakcií, napríklad v smernici o službách, smerniciach o verejnom obstarávaní, revidovanej smernici o DPH (elektronickej fakturácii) a nariadení o iniciatíve európskych občanov. Navrhované nariadenie navyše poskytne právny rámec, ktorý prospeje širokému prijatiu veľkých pilotných opatrení (LSP) zavedených na úrovni EÚ na podporu vývoja interoperabilných a dôveryhodných prostriedkov elektronickej komunikácie (vrátane SPOCS, na podporu implementácie smernice o službách; STORK, na podporu vývoja a používania interoperabilných elektronických identifikácií; PEPPOL, na podporu a používanie interoperabilných riešení elektronického obstarávania; a epSOS, na podporu vývoja a používania interoperabilných riešení elektronického zdravotníctva; eCodex, na podporu vývoja a používania interoperabilných riešení elektronickej justície).

1.6. Trvanie akcie a jej finančného vplyvu

☐ Návrh/iniciatíva s **obmedzeným trvaním**

– ☐ Návrh/iniciatíva sú v platnosti od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finančný vplyv trvá od RRRR do RRRR

☑ Návrh/iniciatíva s **neobmedzeným trvaním**

1.7. Plánovaný spôsob hospodárenia[27]

☑ **Priame centralizované hospodárenie** na úrovni Komisie

[27] Podrobnosti o spôsoboch hospodárenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

☐ **Nepriame centralizované hospodárenie** s delegovaním úloh súvisiacich s plnením rozpočtu na:

– ☐ výkonné agentúry

– ☐ subjekty zriadené spoločenstvami[28]

– ☐ národné verejnoprávne subjekty/subjekty poverené vykonávaním verejnej služby

– ☐ osoby poverené realizáciou osobitných akcií podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte v zmysle článku 49 nariadenia o rozpočtových pravidlách

☐ **Zdieľané hospodárenie** s členskými štátmi

☐ **Decentralizované hospodárenie** s tretími krajinami

☐ **Spoločné hospodárenie** s medzinárodnými organizáciami ***(uveďte)***

V prípade viacerých spôsobov hospodárenia, uveďte v oddiele „Poznámky" presnejšie vysvetlenie.

Poznámky

[//]

[28] Podľa článku 185 nariadenia o rozpočtových pravidlách.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa kontroly a predkladania správ

Uveďte časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Prvé hodnotenie sa uskutoční 4 roky po nadobudnutí účinnosti nariadenia. V nariadení je uvedené osobitné ustanovenie o správe, ktorou Komisia Európsky parlament a Radu oboznámi s jeho uplatňovaním. Následné správy bude potom predkladať každé 4 roky. Použije sa metodika Komisie pre vykonávanie hodnotení. Tieto hodnotenia sa budú realizovať za pomoci cielených štúdií o vykonávaní právnych nástrojov, dotazníkov pre národné orgány, odborných diskusií, workshopov, prieskumov Eurobarometra atď.

2.2. Systémy riadenia a kontroly

2.2.1. Zistené riziká

Bolo vykonané posúdenie vplyvu, ktoré je pripojené k návrhu nariadenia. Novým právnym nástrojom sa stanoví vzájomné uznávanie a akceptovanie elektronickej identifikácie naprieč hranicami, zlepší sa súčasný rámec pre elektronické podpisy, posilní sa národný dohľad nad poskytovateľmi dôveryhodných služieb a zabezpečí sa právny účinok a uznávanie súvisiacich dôveryhodných služieb. Ďalej sa ním zavádza využívanie delegovaných a vykonávacích aktov ako mechanizmu na zabezpečenie pružnosti vzhľadom na technologický vývoj.

2.2.2. Plánované metódy kontroly

Existujúce metódy kontroly uplatňované Komisiou sa vzťahujú na dodatočné rozpočtové prostriedky.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce a plánované preventívne a ochranné opatrenia.

Existujúce metódy prevencie podvodov uplatňované Komisiou sa vzťahujú na dodatočné rozpočtové prostriedky.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Kapitola viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo [Názov……...……]	DRP/ NRP [29]	krajín EZVO[30]	kandidátskych krajín[31]	tretích krajín	v zmysle článku 18 ods. 1 písm. aa) nariadenia o rozpočtových pravidlách
5	09. 01 01 01 Výdavky spojené s pracovníkmi GR Informačná spoločnosť a médiá	NRP	NIE	NIE	NIE	NIE
5	09. 01 02 01 Externí zamestnanci	NRP	NIE	NIE	NIE	NIE

29 DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky

30 EZVO: Európske združenie voľného obchodu.

31 Kandidátske krajiny a prípadne potenciálne kandidátske krajiny západného Balkánu.

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

Okruh viacročného finančného rámca:	**Číslo**	[Okruh 1. **Inteligentný a inkluzívny rast** ……...……]

GR: INFSO			Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok 2018	**Rok 2019**	**Rok 2020**	**SPOLU**
• Operačné rozpočtové prostriedky										
Číslo rozpočtového riadka – neuplatňuje sa	Záväzky	(1)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Platby	(2)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Číslo rozpočtového riadka – neuplatňuje sa	Záväzky	(1a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Platby	(2a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Administratívne rozpočtové prostriedky financované z balíka prostriedkov určených na realizáciu špecifických programov[32]			0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Číslo rozpočtového riadka		(3)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Rozpočtové prostriedky pre GR INFSO SPOLU	Záväzky	=1+1a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Platby	=2+2a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**

[32] Technická a/alebo administratívna pomoc a výdavky určené na financovanie realizácie programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

Okruh viacročného finančného rámca:	**5**	„ Administratívne výdavky “

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**SPOLU**
		GR: INFSO							
• Ľudské zdroje		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Iné administratívne výdavky									
GR INFSO **SPOLU**	Rozpočtové prostriedky	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Rozpočtové prostriedky OKRUHU 5 viacročného finančného rámca SPOLU	(Záväzky spolu = platby spolu)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**SPOLU**
Rozpočtové prostriedky v rámci OKRUHOV 1 až 5 viacročného finančného rámca SPOLU	Záväzky	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Platby	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Odhadovaný vplyv na operačné rozpočtové prostriedky

– ☑ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov

– ☐ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v tabuľke:

3.2.3. Odhadovaný vplyv na administratívne rozpočtové prostriedky

3.2.3.1. Zhrnutie

– ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov.

– ☑ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok **N 2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**SPOLU**
OKRUH 5 viacročného finančného rámca								
Ľudské zdroje	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Iné administratívne výdavky								
Medzisúčet OKRUHU 5 viacročného finančného rámca	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Mimo OKRUHU 5[33] viacročného finančného rámca								
Ľudské zdroje								
Ostatné administratívne výdavky								
Medzisúčet mimo OKRUHU 5 viacročného finančného rámca								

SPOLU	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Technická a/alebo administratívna pomoc a výdavky určené na financovanie realizácie programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.3.2. Odhadované potreby ľudských zdrojov

– ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov
– ☑ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

Odhady sa zaokrúhľujú na celé čísla (alebo najviac na jedno desatinné miesto)

	Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**
• Plán pracovných miest (úradníci a dočasní zamestnanci)							
09 01 01 01 (sídlo a kancelárie zastúpenia Komisie)	9	9	9	9	9	9	9
XX 01 01 02 (Delegácie)							
XX 01 05 01 (Nepriamy výskum)							
10 01 05 01 (Priamy výskum)							
• Externí zamestnanci (ekvivalent jednotiek plného pracovného času)[34]							
09 01 02 01 (CA, INT, SNE z celkového finančného krytia)	3	3	3	3	3	3	3
XX 01 02 02 (CA, INT, JED, LA a SNE v delegáciách)							
XX 01 04 yy[35] - ústredie [36]							
XX 01 04 yy[35] - v delegáciách							
XX 01 05 02 (ZZ, PADZ, VNE – nepriamy výskum)							
10 01 05 02 (ZZ, PADZ, VNE – Priamy výskum)							
Iné rozpočtové riadky (uveďte)							
SPOLU	**12**	**12**	**12**	**12**	**12**	**12**	**12**

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	Riadia legislatívne postupy prijatia plánovaného nariadenia Európskym parlamentom a Radou a súvisiacich delegovaných/vykonávacích aktov. Prioritné oblasti: 1. Vytvorenie nového legislatívneho rámca pre dôveryhodné elektronické služby 2. Podporenie prijatia dôveryhodných elektronických služieb pomocou zvýšenia informovanosti MSP a občanov o ich potenciáli

[34] ZZ = zmluvný zamestnanec; PADZ= pracovníci agentúr dočasného zamestnávania; PED = pomocný expert v delegácii; MZ = miestny zamestnanec; VNE = vyslaný národný expert;

[35] V rámci stropu pre externých zamestnancov z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

[36] Najmä pre štrukturálne fondy, Európsky poľnohospodársky fond pre rozvoj vidieka (EPFRV) a Európsky fond pre rybné hospodárstvo (EFRH).

	3. Nadväzné opatrenie na smernicu 1999/93/ES vrátane medzinárodných aspektov 4. Podporenie veľkých pilotných projektov s cieľom zrýchliť konkrétnu realizáciu cieľa nového legislatívneho rámca.
Externí zamestnanci	Tak, ako sa uvádza vyššie

3.2.4. Súlad s platným viacročným finančným rámcom

– ☑ Návrh/iniciatíva je v súlade s platným viacročným finančným rámcom.

– ☐ Návrh/iniciatíva si vyžaduje zmenu v plánovaní príslušného okruhu vo viacročnom finančnom rámci.

Vysvetlite požadovanú zmenu v plánovaní a uveďte príslušné rozpočtové položky a zodpovedajúce sumy.

– ☐ Návrh/iniciatíva si vyžaduje, aby sa použil nástroj flexibility, alebo aby sa uskutočnila revízia viacročného finančného rámca[37].

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy.

3.2.5. Účasť tretích strán na financovaní

– ☑ Návrh/iniciatíva nebude zahŕňať spolufinancovanie tretími stranami

– ☐ Návrh/iniciatíva bude zahŕňať spolufinancovanie tretími stranami, ako je uvedené v nasledujúcej tabuľke:

3.3. Odhadovaný vplyv na príjmy

– ☑ Návrh/iniciatíva nemá finančný vplyv na príjmy.

– ☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:

- ☐ vplyv na vlastné zdroje
- ☐ vplyv na rôzne príjmy

[37] Pozri body 19 a 24 medziinštitucionálnej dohody.