RADA EVROPSKÉ UNIE

Brusel 7. června 2012 (08.06)
(OR. en)

10977/12

Interinstitucionální spis: 2012/0146 (COD)

TELECOM 122
MI 411
DATAPROTECT 73
CODEC 1576

NÁVRH

Odesílatel:	Evropská komise
Ze dne:	5. června 2012
Č. dok. Komise:	COM(2012) 238 final
Předmět:	Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu

Delegace naleznou v příloze návrh Komise podaný s průvodním dopisem Jordiho AYETA PUIGARNAUA, ředitele, pro Uweho CORSEPIUSE, generálního tajemníka Rady Evropské unie.

Příloha: COM(2012) 238 final

EVROPSKÁ KOMISE

V Bruselu dne 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu

(Text s významem pro EHP)

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

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

Tato důvodová zpráva objasňuje navrhovaný právní rámec, který má zvýšit důvěryhodnost elektronických transakcí na vnitřním trhu.

Budování důvěryhodnosti internetového prostředí má pro hospodářský rozvoj klíčový význam. Nedostatečná důvěra vede k tomu, že se spotřebitelé, podniky a správní orgány zdráhají provádět transakce elektronickými prostředky a přijímat nové služby.

Digitální agenda pro Evropu[1] určuje stávající překážky digitálního rozvoje v Evropě a navrhuje právní předpisy o elektronických podpisech (klíčové opatření 3) a vzájemné uznávání elektronické identifikace a elektronické autentizace (klíčové opatření 16), vytvoření jednoznačného právního rámce s cílem zabránit roztříštěnosti a nedostatečné interoperabilitě, zlepšit digitální občanství a předcházet kyberkriminalitě. Právní předpis zajišťující vzájemné uznávání elektronické identifikace a autentizace v celé EU a přezkum směrnice o elektronických podpisech je rovněž jedním z klíčových opatření v *Aktu o jednotném trhu*[2] k uskutečnění jednotného digitálního trhu. *Plán stability a růstu*[3] vyzdvihuje klíčovou úlohu budoucího společného právního rámce pro vzájemné přeshraniční uznávání a přijímání elektronické identifikace a autentizace při rozvoji digitální ekonomiky.

Navrhovaný právní rámec sestávající z „*nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu*“ se snaží zajistit bezpečné a bezproblémové elektronické kontakty mezi podniky, občany a orgány veřejné správy, a tím zvýšit efektivnost veřejných a soukromých internetových služeb, elektronického podnikání a elektronického obchodu v EU.

Stávající právní předpis EU, a to směrnice 1999/93/ES o „*zásadách Společenství pro elektronické podpisy*“[4], se v zásadě vztahuje pouze na elektronické podpisy. Neexistuje ucelený přeshraniční a meziodvětvový rámec EU pro bezpečné, důvěryhodné a snadno použitelné transakce, který zahrnuje elektronickou identifikaci, autentizaci a podpisy.

Cílem je stávající právní předpisy zlepšit a rozšířit je tak, aby zahrnovaly vzájemné uznávání a přijímání oznámených systémů elektronické identifikace a ostatních nezbytných souvisejících důvěryhodných elektronických služeb na úrovni EU.

2. VÝSLEDKY KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

Tato iniciativa je výsledkem rozsáhlých konzultací ohledně přezkumu stávajícího právního rámce pro elektronické podpisy, v jejichž průběhu získala Komise zpětnou vazbu od členských států, Evropského parlamentu a ostatních zúčastněných stran[5]. Internetová veřejná konzultace byla doplněna „konzultačním panelem pro malé a střední podniky“ s cílem zjistit zvláštní názory a potřeby malých a středních podniků a jinými cílenými konzultacemi se

---

1 KOM(2010) 245 ze dne 19.5.2010.

2 KOM(2011) 206 v konečném znění ze dne 13.4.2011.

3 KOM(2011) 669 ze dne 12.10.2011.

4 Úř. věst. L 13, 19.1.2000, s. 12.

5 Pokud jde o podrobné údaje o konzultaci, viz http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

zúčastněnými stranami[6,7]. Komise zadala rovněž řadu studií týkajících se elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb.

Konzultace objasnily, že velká většina zúčastněných stran souhlasila s tím, že je nutné stávající rámec přezkoumat v zájmu odstranění mezer, které ponechala směrnice o elektronickém podpisu. Mělo se za to, že to bude lépe reagovat na problémy, které vyvolává rychlý rozvoj nových technologií (zejména internetový a mobilní přístup) a rostoucí globalizace, přičemž bude současně zachována technologická neutralita právního rámce.

V souladu se svou politikou zlepšování právní úpravy provedla Komise posouzení dopadů jednotlivých alternativ politiky. Posouzeny byly tři soubory možností politiky, které se zabývaly 1. oblastí působnosti nového rámce, 2. právním nástrojem a 3. úrovní potřebného dohledu[8]. Ukázalo se, že upřednostňovanou možností politiky je zvýšení právní jistoty, posílení koordinace vnitrostátního dohledu, zajištění vzájemného uznávání a přijímání systémů elektronické identifikace a začlenění nezbytných souvisejících důvěryhodných služeb. Posouzení dopadů dospělo k závěru, že toto povede k značnému zvýšení právní jistoty, bezpečnosti a důvěry, pokud jde o přeshraniční elektronické transakce, což bude mít za následek menší roztříštěnost trhu.

3. PRÁVNÍ STRÁNKA NÁVRHU

3.1 Právní základ

Tento návrh je založen na článku 114 SFEU, který se týká přijímání pravidel k odstranění stávajících překážek fungování vnitřního trhu. Občané, podniky a správní orgány budou moci využívat vzájemné přeshraniční uznávání a přijímání elektronické identifikace, autentizace, podpisů a ostatních důvěryhodných služeb, jsou-li tyto zapotřebí pro přístup a provedení elektronických postupů nebo transakcí.

Za nejvhodnější právní nástroj se proto považuje nařízení. Přímá použitelnost nařízení podle článku 288 SFEU odstraní právní nejednotnost a zajistí větší právní jistotu zavedením harmonizovaného souboru základních pravidel přispívajících k fungování vnitřního trhu.

3.2 Subsidiarita a proporcionalita

Aby bylo opatření na úrovni EU odůvodněné, je třeba dodržet zásadu subsidiarity:

a) Nadnárodní charakter problému (ověření potřebnosti)

Nadnárodní povaha elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb vyžaduje opatření na úrovni EU. Samotná domácí (tj. vnitrostátní)

---

6 Dne 10. 3. 2011 se uskutečnil workshop pro zúčastněné strany, jehož se zúčastnili zástupci veřejného i soukromého sektoru a akademické obce, aby projednali, jaká legislativní opatření jsou zapotřebí k odstranění budoucích problémů. Jednalo se o interaktivní fórum pro výměnu názorů, které ukázalo různé postoje k otázkám nadneseným ve veřejné konzultaci. Řada organizací zaslala stanoviska z vlastního podnětu.

7 Polské předsednictví EU uspořádalo dne 9. 11. 2011 ve Varšavě schůzku s členskými státy týkající se elektronického podpisu a dne 17. 11. 2011 schůzku v Poznani týkající se elektronické identifikace. Dne 25. 1. 2012 svolala Komise workshop pro členské státy za účelem projednání zbývajících záležitostí týkajících se elektronické identifikace, autentizace a podpisu.

8 V rámci prvního souboru byly přezkoumány čtyři možnosti: zrušení směrnice o elektronickém podpisu; žádná změna politiky; zvýšení právní jistoty, posílení koordinace vnitrostátního dohledu a zajištění vzájemného uznávání a přijímání elektronické identifikace v celé EU a za čtvrté rozšíření za účelem zahrnutí určitých souvisejících důvěryhodných služeb. Druhý soubor zahrnoval posouzení relativních výhod možností regulace prostřednictvím jednoho nebo dvou nástrojů a prostřednictvím směrnice nebo nařízení. Třetí soubor ověřoval možnosti, které nabízí zavedení vnitrostátních systémů dohledu založených na společných základních požadavcích na dohled v porovnání se systémem dohledu na úrovni EU. Každá možnost politiky byla posouzena s ohledem na její účinnost při dosahování cílů politiky, hospodářské dopady na zúčastněné strany (včetně rozpočtu orgánů EU), sociální a environmentální dopady a vliv na administrativní zátěž, a to s pomocí skupiny, v níž byla zastoupena všechna zúčastněná generální ředitelství Komise.

opatření by nepostačovala ke splnění cílů a nedosáhla by výsledků stanovených ve *strategii Evropa 2020*[9]. Zkušenosti naopak ukazují, že vnitrostátní opatření ve skutečnosti vytvořila překážky interoperability elektronických podpisů v celé Evropě a že v současnosti mají stejný dopad na elektronickou identifikaci, elektronickou autentizaci a související důvěryhodné služby. Je proto nutné, aby EU vytvořila rámec, který umožňuje zabývat se přeshraniční interoperabilitou a zlepšit koordinaci vnitrostátních systémů dohledu. V navrhovaném nařízení se však nelze elektronickou identifikací zabývat stejným všeobecným způsobem jako ostatními důvěryhodnými elektronickými službami, jelikož vydávání prostředků pro identifikaci patří k výsadám jednotlivých členských států. Návrh se proto důsledně zaměřuje pouze na přeshraniční aspekty elektronické identifikace.

Navrhované nařízení vytvoří rovné podmínky pro podniky poskytující důvěryhodné služby, kdy stávající rozdíly ve vnitrostátních právních předpisech v současnosti často vedou k právní nejistotě a dodatečné zátěži. Právní jistota se významně zvýší prostřednictvím jednoznačných povinností týkajících se přijímání kvalifikovaných důvěryhodných služeb ze strany členských států, což vytvoří dodatečnou pobídku pro podniky, aby působily v zahraničí. Pomocí elektronických prostředků se společnost bude například moci zúčastnit veřejné výzvy k předkládání nabídek zveřejněné správními orgány jiného členského státu, aniž by byl její elektronický podpis zablokován kvůli zvláštním vnitrostátním požadavkům a problémům s interoperabilitou. Obdobně bude moci společnost pomocí elektronických prostředků podepisovat smlouvy s protějškem usazeným v jiném členském státě, aniž by se musela obávat různých právních požadavků vztahujících se na důvěryhodné služby, jako jsou elektronické značky, elektronické dokumenty nebo časová razítka. Oznámení o neplnění bude předáno z jednoho členského státu do druhého, přičemž bude zajištěna jeho právní platnost v obou členských státech. Internetový obchod bude důvěryhodnější, budou-li mít kupující k dispozici prostředky pro ověření, že se skutečně nacházejí na internetových stránkách obchodníka podle svého výběru místo na podvodných internetových stránkách.

Vzájemně uznávané prostředky pro elektronickou identifikaci a široce uznávané elektronické podpisy usnadní přeshraniční poskytování četných služeb na vnitřním trhu a podnikům umožní přeshraniční působení, aniž by se při kontaktech s orgány veřejné správy potýkaly s mnoha překážkami. V praxi to bude pro podniky i občany znamenat významné zvýšení efektivnosti při plnění administrativních formalit. Student bude mít například možnost zapsat se pomocí elektronických prostředků na univerzitu v zahraničí, občan bude moci podat daňové přiznání jinému členskému státu prostřednictvím internetu nebo pacient bude mít přístup ke svým zdravotním údajům na internetu. Neexistují-li takovéto vzájemně uznávané prostředky pro elektronickou identifikaci, nemá lékař přístup k údajům o zdravotním stavu pacienta, které jsou zapotřebí k jeho ošetření, a bude nutné opakovat lékařská a laboratorní vyšetření, která již pacient podstoupil.

b) Přidaná hodnota (ověření účinnosti)

Výše nastíněných cílů není v současnosti dosaženo prostřednictvím dobrovolné koordinace mezi členskými státy a ani k tomu pravděpodobně nedojde v budoucnu. To vede k zdvojení úsilí, stanovení rozdílných norem, nadnárodní povaze vedlejších účinků vyvolaných IKT a administrativní složitosti zavedení takovéto koordinace formou dvoustranných a mnohostranných dohod.

Nutnost odstranit tyto problémy, jelikož a) nedostatečná právní jistota kvůli rozdílným vnitrostátním předpisům vyplývajícím z různého výkladu směrnice o elektronickém podpisu a b) nedostatečná interoperabilita systémů pro elektronický podpis, které byly zřízeny na

[9] Sdělení Komise: *Evropa 2020. Strategie pro inteligentní a udržitelný růst podporující začlenění*, KOM(2010) 2020, 3.3.2010.

vnitrostátní úrovni, kvůli nejednotnému uplatňování technických norem vyžaduje koordinaci mezi členskými státy EU, kterou lze účinněji zajistit na úrovni EU.

3.3 Podrobné vysvětlení návrhu

3.3.1 KAPITOLA I – OBECNÁ USTANOVENÍ

Článek 1 stanoví předmět nařízení.

Článek 2 vymezuje věcnou oblast působnosti nařízení.

Článek 3 obsahuje definice pojmů použitých v nařízení. Zatímco některé definice jsou převzaty ze směrnice 1999/93/ES, jiné jsou objasněny, doplněny o dodatečné prvky nebo jsou zavedeny nově.

Článek 4 stanoví zásady vnitřního trhu s ohledem na územní uplatňování nařízení. Výslovně je zmíněno, že nejsou uložená žádná omezení, pokud jde o volný pohyb služeb a volný pohyb zboží.

3.3.2 KAPITOLA II – ELEKTRONICKÁ IDENTIFIKACE

Článek 5 zajišťuje vzájemné uznávání a přijímání prostředků pro elektronickou identifikaci spadajících do systému, jenž bude oznámen Komisi za podmínek stanovených v nařízení. Většina členských států zavedla určitou formu systému elektronické identifikace. Tyto systémy se však v mnoha aspektech liší. Neexistence společného právního základu, který vyžaduje, aby každý členský stát při přístupu k internetovým službám uznával a přijímal prostředky pro elektronickou identifikaci vydané v jiném členském státě, spolu s nedostatečnou přeshraniční interoperabilitou vnitrostátních elektronických identifikací vytváří překážky, které občanům a podnikům brání v plném využívání výhod jednotného digitálního trhu. Tyto právní překážky odstraňuje vzájemné uznávání a přijímání prostředků pro elektronickou identifikaci spadajících do systému oznámeného podle tohoto nařízení.

Nařízení neukládá členským státům povinnost zavést nebo oznámit systémy elektronické identifikace, nýbrž uznávat a přijímat oznámené elektronické identifikace u těch internetových služeb, u nichž se k získání přístupu na vnitrostátní úrovni vyžaduje elektronická identifikace. Případné zvýšení úspor z rozsahu prostřednictvím přeshraničního používání oznámených prostředků pro elektronickou identifikaci a systémů autentizace může členské státy podnítit k tomu, aby oznámily své systémy elektronické identifikace. Článek 6 stanoví pět podmínek pro oznamování systémů elektronické identifikace:

Členské státy mohou oznámit systémy elektronické identifikace, které uznávají v rámci své jurisdikce, pokud se pro přístup k veřejným službám vyžaduje elektronická identifikace. Dalším požadavkem je to, že příslušné prostředky pro elektronickou identifikaci musí být vydány členským státem, který systém oznamuje, jeho jménem nebo alespoň v rámci jeho odpovědnosti.

Členské státy musí zajistit jednoznačné spojení mezi daty pro elektronickou identifikaci a dotčenou osobou. Tato povinnost neznamená, že určitá osoba nemůže mít více prostředků pro elektronickou identifikaci, všechny tyto prostředky však musí souviset s touž osobou.

Spolehlivost elektronické identifikace závisí na dostupnosti prostředků pro autentizaci (tj. možnosti ověřit platnost dat pro elektronickou identifikaci). Nařízení ukládá oznamujícím

členským státům povinnost zajistit bezplatnou autentizaci na internetu vůči třetím osobám. Tato možnost autentizace musí být dostupná nepřetržitě. Stranám spoléhajícím se tuto autentizaci nesmí být uloženy žádné zvláštní technické požadavky, jako je technické zařízení nebo programové vybavení. Toto ustanovení se nevztahuje na požadavky vůči uživatelům (držitelům) prostředků pro elektronickou identifikaci, které jsou z technického hlediska nezbytné pro používání prostředků pro elektronickou identifikaci, jako jsou čtečky karet.

Členské státy musí převzít odpovědnost za jednoznačnost spojení (tj. že data pro identifikaci spojená s určitou osobou nejsou spojena s jinou osobou) a za možnost autentizace (tj. možnost ověřit platnost dat pro elektronickou identifikaci). Odpovědnost členských států se nevztahuje na ostatní aspekty procesu identifikace ani na transakce, které vyžadují identifikaci.

Článek 7 obsahuje pravidla pro oznamování systémů elektronické identifikace Komisi.

Článek 8 má zajistit technickou interoperabilitu oznámených systémů elektronické identifikace prostřednictvím přístupu založeného na koordinaci, včetně aktů v přenesené pravomoci.

3.3.3 KAPITOLA III – DŮVĚRYHODNÉ SLUŽBY

3.3.3.1 Oddíl 1 – Obecná ustanovení

Článek 9 stanoví zásady týkající se odpovědnosti nekvalifikovaných i kvalifikovaných poskytovatelů důvěryhodných služeb. Tento článek vychází z článku 6 směrnice 1999/93/ES a rozšiřuje nárok na náhradu škody způsobené nedbalostí poskytovatele důvěryhodných služeb v důsledku nedodržení dobrých bezpečnostních postupů, které vedlo k narušení bezpečnosti majícímu významný dopad na službu.

Článek 10 popisuje mechanismus pro uznávání a přijímání kvalifikovaných důvěryhodných služeb, které poskytuje poskytovatel usazený ve třetí zemi. Tento článek vychází z článku 7 směrnice 1999/93/ES, ponechává však jedinou prakticky schůdnou možnost, kterou je umožnit toto uznávání na základě mezinárodní dohody mezi Evropskou unií a třetími zeměmi nebo mezinárodními organizacemi.

Článek 11 stanoví zásady ochrany údajů a minimalizace množství údajů. Tento článek vychází z článku 8 směrnice 1999/93/ES.

Článek 12 zajišťuje přístupnost důvěryhodných služeb pro osoby se zdravotním postižením.

3.3.3.2 Oddíl 2 – Dohled

Článek 13 ukládá na základě čl. 3 odst. 3 směrnice 1999/93/ES členským státům povinnost zřídit orgány dohledu a objasňuje a rozšiřuje jejich působnost, pokud jde o poskytovatele důvěryhodných služeb i kvalifikované poskytovatele důvěryhodných služeb.

Článek 14 zavádí explicitní mechanismus vzájemné pomoci mezi orgány dohledu v členských státech s cílem usnadnit přeshraniční dohled nad poskytovateli důvěryhodných služeb. Zavádí pravidla týkající se společných operací a práva orgánů dohledu účastnit se těchto operací.

Článek 15 ukládá kvalifikovaným i nekvalifikovaným poskytovatelům důvěryhodných služeb povinnost zavést odpovídající technická a organizační opatření k zajištění bezpečnosti jejich činností. Příslušné orgány dohledu a jiné relevantní orgány musí být mimoto informovány

o případném narušení bezpečnosti. V případě potřeby orgány dohledu vyrozumí orgány dohledu v ostatních členských státech a přímo nebo prostřednictvím dotyčného poskytovatele důvěryhodných služeb budou informovat veřejnost.

Článek 16 stanoví podmínky pro dohled nad kvalifikovanými poskytovateli důvěryhodných služeb a kvalifikovanými důvěryhodnými službami, které poskytují. Tento článek ukládá kvalifikovaným poskytovatelům důvěryhodných služeb zejména povinnost podrobit se každoročně auditu ze strany uznaného nezávislého subjektu, aby bylo orgánu dohledu potvrzeno, že poskytovatelé plní povinnosti stanovené v nařízení. Ustanovení čl. 16 odst. 2 mimoto přiznává orgánu dohledu právo provést u kvalifikovaných poskytovatelů důvěryhodných služeb kdykoli kontrolu na místě. Orgán dohledu je zmocněn rovněž k vydávání závazných pokynů kvalifikovaným poskytovatelům důvěryhodných služeb, aby přiměřeně napravili případné neplnění povinností, jež bylo zjištěno při bezpečnostním auditu.

Článek 17 se týká kontroly provedené orgánem dohledu na žádost poskytovatele důvěryhodných služeb, který chce začít poskytovat kvalifikované důvěryhodné služby.

Článek 18 ukládá povinnost vyhotovit důvěryhodné seznamy[10], které obsahují informace o kvalifikovaných poskytovatelích důvěryhodných služeb, kteří podléhají dohledu, a o poskytovaných kvalifikovaných službách. Tyto informace musí být prostřednictvím společné šablony zpřístupněny veřejnosti, aby se usnadnilo jejich automatické používání a zajistila náležitá úroveň podrobnosti.

Článek 19 stanoví požadavky, které musí splňovat kvalifikovaní poskytovatelé důvěryhodných služeb, aby byli uznáni jako takoví. Tento článek vychází z přílohy II směrnice 1999/93/ES.

3.3.3.3 Oddíl 3 – Elektronický podpis

Článek 20 stanoví pravidla týkající se právního účinku elektronických podpisů fyzických osob. Tento článek objasňuje a rozšiřuje článek 5 směrnice 1999/93/ES zavedením výslovné povinnosti přiznávat kvalifikovaným elektronickým podpisům stejný právní účinek jako vlastnoručním podpisům. Členské státy musí mimoto zajistit přeshraniční uznávání kvalifikovaných elektronických podpisů v souvislosti s poskytováním veřejných služeb a nesmí zavést dodatečné požadavky, jež by mohly vést k překážkám při používání těchto podpisů.

Článek 21 stanoví požadavky na kvalifikované certifikáty pro elektronický podpis. Objasňuje přílohu I směrnice 1999/93/ES a odstraňuje ustanovení, která v praxi nefungovala (např. omezení týkající se hodnoty transakcí).

Článek 22 stanoví požadavky na kvalifikované prostředky pro vytváření elektronického podpisu. Objasňuje požadavky vztahující se na prostředky pro bezpečné vytváření elektronického podpisu stanovené v čl. 3 odst. 5 směrnice 1999/93/ES, jež je nyní nutno považovat za kvalifikované prostředky pro vytváření elektronického podpisu podle tohoto nařízení. Tento článek rovněž objasňuje, že působnost prostředku pro vytváření elektronického podpisu může být mnohem širší než pouze jako prostředku, který obsahuje data pro vytváření podpisu. Komise může rovněž vyhotovit seznam referenčních čísel norem pro bezpečnostní požadavky vztahující se na tyto prostředky.

[10] Základem pro nové rozhodnutí Komise o důvěryhodných seznamech podle tohoto nařízení je důvěryhodný seznam zavedený rozhodnutím Komise 2009/767/ES ve znění rozhodnutí Komise 2010/425/EU.

Článek 23 zavádí v návaznosti na čl. 3 odst. 4 směrnice 1999/93/ES koncepci certifikace kvalifikovaných prostředků pro vytváření elektronického podpisu za účelem stanovení jejich shody s bezpečnostními požadavky uvedenými v příloze II. Tyto prostředky musí být všemi členskými státy uznány jako prostředky splňující příslušné požadavky, pokud postup certifikace provede certifikační orgán určený členským státem. Komise zveřejní pozitivní seznam těchto certifikovaných prostředků podle článku 24. Komise může rovněž vyhotovit seznam referenčních čísel norem pro posuzování bezpečnosti produktů informačních technologií, jak je uvedeno v čl. 23 odst. 1.

Článek 24 se týká zveřejnění seznamu kvalifikovaných prostředků pro vytváření elektronického podpisu Komisí po oznámení shody ze strany členských států.

Článek 25 navazuje na doporučení uvedená v příloze IV směrnice 1999/93/ES ke stanovení závazných požadavků na ověřování kvalifikovaných elektronických podpisů za účelem zvýšení právní jistoty tohoto ověření.

Článek 26 stanoví podmínky pro kvalifikované služby pro ověřování.

Článek 27 stanoví podmínky pro dlouhodobé uchovávání kvalifikovaných elektronických podpisů. To je možné v důsledku používání postupů a technologií, které jsou s to zajistit důvěryhodnost dat pro ověřování kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti, kdy pro pachatele kybernetických trestných činů může být snadné padělání.

3.3.3.4 Oddíl 4 – Elektronické značky

Článek 28 se týká právního účinku elektronických značek právnických osob. U kvalifikované elektronické značky platí zvláštní právní domněnka, která zaručuje původ a integritu elektronických dokumentů, s nimiž je spojena.

Článek 29 stanoví požadavky na kvalifikované certifikáty pro elektronické značky.

Článek 30 stanoví požadavky na kvalifikované prostředky pro vytváření elektronické značky a jejich certifikaci a zveřejnění seznamu těchto prostředků.

Článek 31 stanoví podmínky pro ověřování a uchovávání kvalifikovaných elektronických značek.

3.3.3.5 Oddíl 5 – Elektronické časové razítko

Článek 32 se týká právního účinku elektronických časových razítek. U kvalifikovaného elektronického časového razítka platí zvláštní právní domněnka ohledně spolehlivosti časového okamžiku.

Článek 33 stanoví požadavky na kvalifikovaná elektronická časová razítka.

3.3.3.6 Oddíl 6 – Elektronické dokumenty

Článek 34 se týká právních účinků a podmínek přijímání elektronických dokumentů. U elektronického dokumentu podepsaného kvalifikovaným elektronickým podpisem nebo opatřeného kvalifikovanou elektronickou značkou platí zvláštní právní domněnka ohledně jeho pravosti a integrity. Co se týká přijímání elektronických dokumentů, pokud se pro

poskytnutí veřejné služby požaduje originální dokument nebo ověřená kopie, přijímají se v ostatních členských státech bez dodatečných požadavků alespoň elektronické dokumenty, které jsou vydány osobami oprávněnými k vydávání příslušných dokumentů a které se podle vnitrostátních právních předpisů členského státu původu považují za originály nebo ověřené kopie.

3.3.3.7 Oddíl 7 – Elektronické doručování

Článek 35 se týká právního účinku dat odeslaných nebo obdržených prostřednictvím elektronického doručování. U kvalifikovaných služeb elektronického doručování je zaručena zvláštní právní domněnka ohledně integrity odesílaných nebo přijímaných dat a spolehlivosti časového okamžiku, k němuž jsou data odeslána nebo obdržena. Tento článek zajišťuje rovněž vzájemné uznávání kvalifikovaných služeb elektronického doručování na úrovni EU.

Článek 36 stanoví požadavky na kvalifikované služby elektronického doručování.

3.3.3.8 Oddíl 8 – Ověřování webových stránek

Tento oddíl má zajistit zaručení pravosti webových stránek, pokud jde o jejich vlastníka.

Článek 37 stanoví požadavky na kvalifikované certifikáty pro ověřování webových stránek, které lze použít k zaručení pravosti webové stránky. Kvalifikovaný certifikát pro ověřování webových stránek poskytuje minimální soubor důvěryhodných informací o webových stránkách a o právní existenci jejich vlastníka.

3.3.4 KAPITOLA IV – AKTY V PŘENESENÉ PRAVOMOCI

Článek 38 obsahuje standardní ustanovení o výkonu přenesených pravomocí v souladu s článkem 290 SFEU (akty v přenesené pravomoci). Tento článek umožňuje zákonodárci přenést na Komisi pravomoc přijímat nelegislativní akty s obecnou působností, kterými se doplňují nebo mění některé prvky legislativního aktu, které nejsou podstatné.

3.3.5 KAPITOLA V – PROVÁDĚCÍ AKTY

Článek 39 obsahuje ustanovení týkající se postupu projednávání ve výboru potřebného pro svěření prováděcích pravomocí Komisi v případech, kdy jsou podle článku 291 SFEU pro provedení právně závazných aktů Unie nezbytné jednotné podmínky. Použije se přezkumný postup.

3.3.6 KAPITOLA VI – ZÁVĚREČNÁ USTANOVENÍ

Článek 40 ukládá Komisi povinnost týkající se hodnocení nařízení a předkládání zpráv o jejích zjištěních.

Článek 41 zrušuje směrnici 1999/93/ES a zajišťuje bezproblémový přechod stávající infrastruktury pro elektronický podpis na nové požadavky stanovené v nařízení.

Článek 42 stanoví datum vstupu nařízení v platnost.

4. ROZPOČTOVÉ DŮSLEDKY

Konkrétní rozpočtové důsledky návrhu vyplývají z úkolů přenesených na Evropskou komisi, jak je uvedeno v legislativním finančním výkazu připojeném k tomuto návrhu.

Návrh nemá dopad na provozní výdaje.

Legislativní finanční výkaz připojený k návrhu nařízení obsahuje rozpočtové důsledky pro samotné nařízení.

2012/0146 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[11],

po konzultaci s evropským inspektorem ochrany údajů[12],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Budování důvěryhodnosti internetového prostředí má pro hospodářský rozvoj klíčový význam. Nedostatečná důvěra vede k tomu, že se spotřebitelé, podniky a správní orgány zdráhají provádět transakce elektronickými prostředky a přijímat nové služby.

(2) Toto nařízení má zvýšit důvěryhodnost elektronických transakcí na vnitřním trhu tím, že umožní, aby mezi podniky, občany a orgány veřejné správy docházelo k bezpečným a bezproblémovým elektronickým kontaktům, a tudíž zvýšit efektivnost veřejných a soukromých internetových služeb, elektronického podnikání a elektronického obchodu v Unii.

(3) Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy[13] se v zásadě vztahovala pouze na elektronické podpisy, aniž by poskytovala ucelený přeshraniční a meziodvětvový rámec pro bezpečné, důvěryhodné a snadno použitelné elektronické transakce. Toto nařízení *acquis* směrnice zlepšuje a rozšiřuje.

---

11 Úř. věst. C , , s. .

12 Úř. věst. C , s. .

13 Úř. věst. L 13, 19.1.2000, s. 12.

(4) Ve sdělení Komise s názvem Digitální agenda pro Evropu[14] byly jako hlavní překážky účinného cyklu digitální ekonomiky určeny roztříštěnost digitálního trhu, nedostatečná interoperabilita a nárůst kyberkriminality. Ve své zprávě o občanství za rok 2010 vyzdvihla Komise potřebu odstranit hlavní problémy, které evropským občanům brání ve využívání výhod jednotného digitálního trhu a přeshraničních digitálních služeb[15].

(5) Evropská rada Komisi vyzvala, aby vytvořila do roku 2015 jednotný digitální trh[16] s cílem urychleně pokročit v klíčových oblastech digitálního hospodářství a aby prosazovala plně integrovaný jednotný digitální trh[17] usnadněním přeshraničního využívání internetových služeb, přičemž je zvláštní pozornost věnována usnadnění bezpečné elektronické identifikace a autentizace.

(6) Rada Komisi vyzvala, aby přispěla k jednotnému digitálnímu trhu vytvořením vhodných podmínek pro vzájemné přeshraniční uznávání klíčových předpokladů, jako je elektronická identifikace, elektronické dokumenty, elektronické podpisy a elektronické doručování, a pro interoperabilní služby elektronické veřejné správy v celé Evropské unii[18].

(7) Evropský parlament zdůraznil význam bezpečnosti elektronických služeb, zejména elektronických podpisů, a nutnost vytvořit na celoevropské úrovni infrastrukturu veřejných klíčů, a vyzval Komisi, aby zřídila portál evropských evidenčních orgánů s cílem zajistit přeshraniční interoperabilitu elektronických podpisů a zvýšit bezpečnost transakcí prováděných po internetu[19].

(8) Směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu[20] vyžaduje, aby členské státy vytvořily jednotná kontaktní místa s cílem zajistit, aby veškeré postupy a formality vztahující se k přístupu k činnosti poskytování služeb a jejímu výkonu mohly být snadno splněny na dálku a pomocí elektronických prostředků, a to prostřednictvím příslušného jednotného kontaktního místa a u příslušných orgánů. Mnoho internetových služeb přístupných prostřednictvím jednotného kontaktního místa vyžaduje elektronickou identifikaci, autentizaci a podpis.

(9) Poskytovatelé služeb z jiného členského státu nemohou ve většině případů použít pro přístup k těmto službám svou elektronickou identifikaci, jelikož vnitrostátní systémy elektronické identifikace v jejich zemi nejsou uznávány a přijímány v ostatních členských státech. Tato elektronická bariéra znemožňuje, aby poskytovatelé služeb plně využívali výhod vnitřního trhu. Vzájemně uznávané a přijímané prostředky pro elektronickou identifikaci usnadní přeshraniční poskytování četných služeb na vnitřním trhu a umožní podnikům přeshraniční působení, aniž by se při kontaktech s orgány veřejné správy potýkaly s mnoha překážkami.

---

14 KOM(2010) 245 v konečném znění/2.

15 Zpráva o občanství EU za rok 2010: Odstranit překážky pro výkon práv občanů EU, KOM(2010) 603 v konečném znění, bod 2.2.2, s. 12.

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

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

18 Závěry Rady o Evropském akčním plánu „eGovernment“ na období 2011–2015; 3093. zasedání Rady ve složení pro dopravu, telekomunikace a energetiku, Brusel, 27. května 2011.

19 Usnesení Evropského parlamentu ze dne 21. září 2010 o dotvoření vnitřního trhu pro elektronický obchod, 21.9.10, P7_TA(2010)0320 a usnesení Evropského parlamentu ze dne 15. června 2010 o řízení internetu: další kroky, P7_TA(2010)0208.

20 Úř. věst. L 376, 27.12.2006, s. 36.

(10) Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči[21] zřizuje síť vnitrostátních orgánů odpovědných za elektronické zdravotnictví. V zájmu zvýšení bezpečnosti a zajištění kontinuity přeshraniční zdravotní péče musí síť vypracovat pokyny k přeshraničnímu přístupu k elektronickým zdravotním údajům a službám, včetně podpory „*společných opatření pro identifikaci a ověřování za účelem snadnější přenositelnosti údajů v rámci přeshraniční zdravotní péče*“. Vzájemné uznávání a přijímání elektronické identifikace a autentizace je hlavním předpokladem pro to, aby se přeshraniční zdravotní péče stala pro evropské občany skutečností. Pokud občané cestují za účelem lékařského ošetření, údaje o jejich zdravotním stavu musí být dostupné v zemi, v níž je léčba poskytnuta. To vyžaduje pevný, bezpečný a důvěryhodný rámec pro elektronickou identifikaci.

(11) Jedním z cílů tohoto nařízení je odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají pro přístup alespoň k veřejným službám. Toto nařízení nemá zasahovat do systémů správy elektronické identity a souvisejících infrastruktur zřízených v členských státech. Toto nařízení má zajistit, aby u přístupu k přeshraničním internetovým službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace.

(12) Pro účely elektronické identifikace by měly mít členské státy možnost používat nebo zavést prostředky pro přístup k internetovým službám. Členské státy by měly mít rovněž možnost rozhodnout, zda do poskytování těchto prostředků zapojí soukromý sektor. Členské státy by neměly mít povinnost oznámit své systémy elektronické identifikace. Je na členských státech, aby si zvolily, zda oznámí veškeré nebo pouze některé systémy elektronické identifikace používané na vnitrostátní úrovni pro přístup alespoň k veřejným internetovým službám či zvláštním službám, nebo zda tyto systémy neoznámí.

(13) V nařízení je nutno stanovit určité podmínky, pokud jde o to, které prostředky pro elektronickou identifikaci musí být přijímány, a způsob oznamování systémů. Tyto podmínky by měly členským státům pomoci při budování nezbytné vzájemné důvěry v systémy elektronické identifikace a při vzájemném uznávání a přijímání prostředků pro elektronickou identifikaci spadajících do jejich oznámených systémů. Zásada vzájemného uznávání a přijímání by se měla použít v případě, splní-li oznamující členský stát podmínky pro oznámení a bylo-li oznámení zveřejněno v *Úředním věstníku Evropské unie*. Přístup k těmto internetovým službám a jejich skutečné poskytnutí žadateli by však mělo úzce souviset s právem na obdržení takovýchto služeb za podmínek stanovených ve vnitrostátních právních předpisech.

(14) Členské státy by měly mít možnost rozhodnout, zda do vydávání prostředků pro elektronickou identifikaci zapojí veřejný sektor, a umožnit, aby soukromý sektor používal pro účely identifikace prostředky pro elektronickou identifikaci v rámci oznámeného systému, je-li to zapotřebí u internetových služeb nebo elektronických transakcí. Možnost používat tyto prostředky pro elektronickou identifikaci by soukromému sektoru umožnila spoléhat se na elektronickou identifikaci a autentizaci, která se již v mnoha členských státech ve značné míře používá přinejmenším u veřejných služeb, a usnadnila by podnikům a občanům přeshraniční přístup

[21] Úř. věst. L 88, 4.4.2011, s. 45.

k internetovým službám. V zájmu snazšího přeshraničního používání těchto prostředků pro elektronickou identifikaci soukromým sektorem by měla být pro spoléhající se strany dostupná možnost autentizace zajištěná členskými státy, aniž by se rozlišovalo mezi veřejným nebo soukromým sektorem.

(15) Přeshraniční používání prostředků pro elektronickou identifikaci v rámci oznámeného systému vyžaduje, aby členské státy spolupracovaly při zajišťování technické interoperability. To vylučuje případné zvláštní vnitrostátní technické předpisy, které vyžadují, aby si strany z jiných členských států musely pořídit například zvláštní technické zařízení nebo programové vybavení k ověřování a potvrzení platnosti oznámené elektronické identifikace. Na druhou stranu jsou nevyhnutelné technické požadavky vztahující se na uživatele, které vyplývají ze specifikací používaného tokenu (např. inteligentní karty).

(16) Spolupráce členských států by měla zajistit technickou interoperabilitu oznámených systémů elektronické identifikace v zájmu posílení vysoké úrovně důvěryhodnosti a bezpečnosti odpovídající míře rizika. Této spolupráci by měla napomoci výměna informací a sdílení osvědčených postupů mezi členskými státy za účelem jejich vzájemného uznávání.

(17) Toto nařízení by mělo stanovit rovněž obecný právní rámec pro využívání důvěryhodných elektronických služeb. Nemělo by však ukládat obecnou povinnost používat tyto služby. Toto nařízení by se zejména nemělo vztahovat na poskytování služeb na základě dobrovolných dohod podle soukromého práva. Nemělo by se vztahovat ani na aspekty související s uzavíráním a platností smluv nebo jiných právních závazků, pokud existují požadavky na formu předepsané vnitrostátními právními předpisy nebo právními předpisy Unie.

(18) V zájmu přispění k obecnému přeshraničnímu využívání důvěryhodných elektronických služeb by mělo být možné použít je ve všech členských státech jako důkaz v soudním řízení.

(19) Členské státy by měly mít možnost stanovit kromě důvěryhodných služeb, jež jsou součástí uzavřeného seznamu důvěryhodných služeb stanoveného v tomto nařízení, i jiné druhy důvěryhodných služeb za účelem jejich uznávání na vnitrostátní úrovni jako kvalifikovaných důvěryhodných služeb.

(20) Vzhledem k tempu technologických změn by toto nařízení mělo přijmout přístup, který je otevřený inovacím.

(21) Toto nařízení by mělo být z technologického hlediska neutrální. Právních účinků, které přiznává, by mělo být možné dosáhnout jakýmikoli technickými prostředky, jsou-li splněny požadavky tohoto nařízení.

(22) K zvýšení důvěry občanů ve vnitřní trh a na podporu používání důvěryhodných služeb a produktů by měly být zavedeny pojmy „kvalifikované důvěryhodné služby“ a „kvalifikovaný poskytovatel důvěryhodných služeb“ za účelem stanovení požadavků a povinností, které mají zajistit vysokou úroveň bezpečnosti všech používaných nebo poskytovaných kvalifikovaných důvěryhodných služeb a produktů.

(23) V souladu se závazky podle Úmluvy OSN o právech osob se zdravotním postižením, která v EU vstoupila v platnost, musí mít osoby se zdravotním postižením možnost

využívat poskytované důvěryhodné služby a konečné uživatelské produkty používané při poskytování těchto služeb stejně jako ostatní spotřebitelé.

(24) Poskytovatel důvěryhodných služeb je správcem osobních údajů, a musí proto dodržovat povinnosti stanovené ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[22]. Zejména je třeba omezit sběr údajů na nejnižší možnou úroveň s přihlédnutím k účelu poskytované služby.

(25) Orgány dohledu by měly spolupracovat s orgány pro ochranu údajů a vyměňovat si s nimi informace, aby bylo zajištěno řádné uplatňování právních předpisů v oblasti ochrany údajů ze strany poskytovatelů služeb. Tato výměna údajů by se měla týkat zejména bezpečnostních incidentů a narušení bezpečnosti osobních údajů.

(26) Všichni poskytovatelé důvěryhodných služeb by měli uplatňovat dobré bezpečnostní postupy, které jsou přiměřené s ohledem na rizika spojená s jejich činnostmi, aby byla posílena důvěra uživatelů v jednotný trh.

(27) Ustanovení o používání pseudonymů v certifikátech by neměla členským státům bránit v tom, aby vyžadovaly identifikaci osob podle právních předpisů Unie nebo podle vnitrostátních právních předpisů.

(28) Všechny členské státy by měly dodržovat společné základní požadavky na dohled s cílem zajistit srovnatelnou úroveň bezpečnosti kvalifikovaných důvěryhodných služeb. K usnadnění jednotného uplatňování těchto požadavků v celé Unii by členské státy měly přijmout srovnatelné postupy a měly by si vyměňovat informace o svých činnostech v oblasti dohledu a o osvědčených postupech používaných v praxi.

(29) Za účelem poskytování náležitých informací dotčeným stranám v případě narušení bezpečnosti nebo ztráty integrity je nezbytné oznamování narušení bezpečnosti a posuzování bezpečnostních rizik.

(30) Aby mohla Komise a členské státy posoudit účinnost mechanismu pro oznamování narušení bezpečnosti, který je zaveden tímto nařízením, měly by orgány dohledu poskytovat souhrnné informace Komisi a Evropské agentuře pro bezpečnost sítí a informací (ENISA).

(31) Aby mohla Komise a členské státy posoudit dopady tohoto nařízení, měly by orgány dohledu poskytovat statistické údaje o kvalifikovaných důvěryhodných službách a o jejich využívání.

(32) Aby mohla Komise a členské státy posoudit účinnost zdokonaleného mechanismu dohledu, který je zaveden tímto nařízením, měly by orgány dohledu podávat zprávy o své činnosti. To by napomohlo při usnadňování výměny osvědčených postupů mezi orgány dohledu a zajistilo ověření toho, zda jsou ve všech členských státech jednotně a účinně uplatňovány základní požadavky na dohled.

(33) K zajištění udržitelnosti a stálosti kvalifikovaných důvěryhodných služeb a posílení důvěry uživatelů v kontinuitu kvalifikovaných důvěryhodných služeb by orgány dohledu měly zajistit, aby byly po příslušnou dobu uchovávány údaje

[22] Úř. věst. L 281, 23.11.1995, s. 31.

o kvalifikovaných poskytovatelích důvěryhodných služeb a aby byly přístupné i v případě, že kvalifikovaný poskytovatel důvěryhodných služeb přestane existovat.

(34) K usnadnění dohledu nad kvalifikovanými poskytovateli důvěryhodných služeb například v případě, že poskytovatel poskytuje své služby na území jiného členského státu a nepodléhá v tomto státě dohledu nebo pokud se počítače poskytovatele nacházejí na území jiného členského státu, než ve kterém je usazen, by měl být zřízen systém vzájemné pomoci mezi orgány dohledu v členských státech.

(35) Poskytovatelé důvěryhodných služeb odpovídají za dodržování požadavků stanovených v tomto nařízení při poskytování důvěryhodných služeb, zejména kvalifikovaných důvěryhodných služeb. Orgány dohledu odpovídají za dohled nad dodržováním těchto požadavků ze strany poskytovatelů důvěryhodných služeb.

(36) S cílem umožnit účinný postup pro zahájení poskytování služeb, který by měl vést k zařazení kvalifikovaných poskytovatelů důvěryhodných služeb a kvalifikovaných důvěryhodných služeb, které poskytují, na důvěryhodné seznamy, je nutno podporovat předběžné kontakty mezi potencionálními kvalifikovanými poskytovateli důvěryhodných služeb a příslušným orgánem dohledu v zájmu usnadnění hloubkové kontroly vedoucí k poskytování kvalifikovaných důvěryhodných služeb.

(37) Nezbytnými prvky při budování důvěry mezi tržními subjekty jsou důvěryhodné seznamy, jelikož udávají stav kvalifikace poskytovatele služeb v době dohledu, na druhou stranu nejsou podmínkou pro dosažení stavu kvalifikace a poskytování kvalifikovaných důvěryhodných služeb, jež vyplývá z dodržování požadavků tohoto nařízení.

(38) Jakmile byla kvalifikovaná důvěryhodná služba oznámena, nemůže být s ohledem na splnění správního postupu nebo formality dotčeným subjektem z veřejného sektoru odmítnuta kvůli tomu, že není zařazena na důvěryhodné seznamy vyhotovené členskými státy. Za tímto účelem subjekt z veřejného sektoru odkazuje na orgán veřejné správy či jiný subjekt pověřený poskytováním služeb elektronické veřejné správy, jako je podávání daňového přiznání prostřednictvím internetu, žádosti o rodné listy, účast v postupech elektronického zadávání veřejných zakázek atd.

(39) Ačkoliv k zajištění vzájemného uznávání elektronických podpisů je zapotřebí vysoká úroveň bezpečnosti, měly by být ve zvláštních případech, například v rámci rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu[23], přijímány rovněž elektronické podpisy s nižší zárukou bezpečnosti.

(40) Podepisující osoba by měla mít možnost svěřit kvalifikované prostředky pro vytváření elektronického podpisu do péče třetí straně, pokud jsou zavedeny odpovídající mechanismy a postupy, které zajišťují, že podepisující osoba má výhradní kontrolu nad používáním svých dat pro vytváření elektronického podpisu, a použitím tohoto prostředku jsou splněny požadavky na kvalifikovaný podpis.

[23] Úř. věst. L 274, 20.10.2009, s. 36.

(41) V zájmu zajištění právní jistoty ohledně platnosti podpisu je nezbytné podrobně uvést, které prvky kvalifikovaného elektronického podpisu musí posoudit spoléhající se strana, která provádí ověření. Stanovení požadavků na kvalifikované poskytovatele důvěryhodných služeb, kteří mohou poskytovat kvalifikovanou službu pro ověřování spoléhajícím se stranám, jež nejsou ochotny nebo schopny provádět ověřování kvalifikovaných elektronických podpisů samy, by mělo soukromý nebo veřejný sektor podnítit k investicím do těchto služeb. Oba prvky by měly usnadnit ověřování kvalifikovaných elektronických podpisů a být vhodné pro všechny strany na úrovni Unie.

(42) Vyžaduje-li transakce kvalifikovanou elektronickou značku právnické osoby, měl by být stejně tak přijatelný kvalifikovaný elektronický podpis zplnomocněného zástupce této právnické osoby.

(43) Elektronické značky by měly sloužit jako důkaz toho, že elektronický dokument vydala určitá právnická osoba, a poskytovat jistotu ohledně původu a integrity dokumentu.

(44) Toto nařízení by mělo zajistit dlouhodobé uchovávání informací, tj. právoplatnost elektronického podpisu a elektronických značek po delší dobu, což zaručuje, že mohou být ověřeny bez ohledu na budoucí technologické změny.

(45) V zájmu většího přeshraničního využívání elektronických dokumentů by toto nařízení mělo stanovit právní účinek elektronických dokumentů, jež by se měly považovat za rovnocenné dokumentům v papírové podobě v závislosti na posouzení rizik a v případě, že je zajištěna pravost a integrita dokumentů. Pro další rozvoj přeshraničních elektronických transakcí na vnitřním trhu je rovněž důležité, aby byly originální elektronické dokumenty nebo ověřené kopie vydané příslušnými subjekty v určitém členském státě podle jeho vnitrostátních právních předpisů přijímány jako takové rovněž v ostatních členských státech. Tímto nařízením by nemělo být dotčeno právo členských států určit, co na vnitrostátní úrovni představuje originál nebo kopii, nařízení však zajišťuje, že je lze jako takové používat rovněž na přeshraničním základě.

(46) Jelikož v současnosti používají příslušné orgány v členských státech při podepisování svých dokumentů elektronickými prostředky různé formáty zaručených elektronických podpisů, je nutné zajistit, aby členské státy mohly při přijímání dokumentů, které byly podepsány elektronickými prostředky, technicky podporovat alespoň určitý počet formátů zaručených elektronických podpisů. Pokud příslušné orgány v členských státech používají zaručené elektronické značky, bude obdobně nutné zajistit, aby podporovaly přinejmenším určitý počet formátů zaručených elektronických značek.

(47) Kromě ověření pravosti dokumentu vydaného právnickou osobou lze elektronické značky použít k ověřování pravosti jakýchkoli digitálních aktiv dotyčné právnické osoby, například softwarového kódu, serverů.

(48) Možnost ověřovat webové stránky a totožnost osoby, která je vlastní, ztíží padělání webových stránek, a tudíž omezí podvody.

(49) Za účelem pružného a rychlého doplnění určitých podrobných technických aspektů tohoto nařízení by měla být Komisi svěřena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, pokud jde o interoperabilitu

elektronických identifikací; bezpečnostní opatření vyžadovaná od poskytovatelů důvěryhodných služeb; uznané nezávislé subjekty odpovědné za provádění auditů u poskytovatelů služeb; důvěryhodné seznamy; požadavky týkající se úrovní bezpečnosti elektronických podpisů; požadavky na kvalifikované certifikáty pro elektronické podpisy, jejich ověřování a uchovávání; orgány odpovědné za certifikaci kvalifikovaných prostředků pro vytváření elektronického podpisu a požadavky týkající se úrovní bezpečnosti elektronických značek a požadavky na kvalifikované certifikáty pro elektronické značky; interoperabilitu mezi doručovacími službami. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni.

(50) Při přípravě a vypracování aktů v přenesené pravomoci by Komise měla zajistit, aby byly příslušné dokumenty předány současně, včas a vhodným způsobem Evropskému parlamentu a Radě.

(51) V zájmu zajištění jednotných podmínek pro provádění tohoto nařízení je třeba svěřit Komisi prováděcí pravomoci, zejména za účelem určení referenčních čísel norem, které vedou k předpokladu shody s určitými požadavky stanovenými v tomto nařízení nebo vymezenými v aktech v přenesené pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí[24].

(52) Z důvodu právní jistoty a jasnosti by měla být směrnice 1999/93/ES zrušena.

(53) V zájmu zajištění právní jistoty pro tržní subjekty, které již používají kvalifikovaná osvědčení vydaná podle směrnice 1999/93/ES, je nutné stanovit dostatečně dlouhé časové období za účelem přechodu. Je rovněž nezbytné umožnit Komisi přijímání prováděcích aktů a aktů v přenesené pravomoci před tímto dnem.

(54) Jelikož cílů tohoto nařízení nemůže být uspokojivě dosaženo na úrovni členských států, a proto jich může být z důvodu rozsahu opatření lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení uvedeného cíle, zejména pokud jde o úlohu Komise jakožto koordinátora činností jednotlivých členských států,

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

1. Toto nařízení stanoví pravidla pro elektronickou identifikaci a důvěryhodné elektronické služby pro elektronické transakce za účelem zajištění řádného fungování vnitřního trhu.

[24] Úř. věst. L 55, 28.2.2011, s. 13.

2. Toto nařízení stanoví podmínky, za nichž členské státy uznávají a přijímají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu.

3. Toto nařízení stanoví právní rámec pro elektronické podpisy, elektronické značky, elektronická časová razítka, elektronické dokumenty, elektronické doručování a ověřování webových stránek.

4. Toto nařízení zajišťuje, aby se důvěryhodné služby a produkty, které vyhovují tomuto nařízení, mohly volně pohybovat na vnitřním trhu.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na elektronickou identifikaci zajišťovanou členskými státy, jejich jménem nebo v rámci jejich odpovědnosti a poskytovateli důvěryhodných služeb usazenými v Unii.

2. Toto nařízení se nevztahuje na poskytování důvěryhodných elektronických služeb na základě dobrovolných dohod podle soukromého práva.

3. Toto nařízení se nevztahuje na aspekty související s uzavíráním a platností smluv či jiných právních závazků, pokud existují požadavky na formu předepsané vnitrostátními právními předpisy nebo právními předpisy Unie.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1. „elektronickou identifikací“ proces používání osobních identifikačních údajů v elektronické podobě, které jednoznačně označují určitou fyzickou nebo právnickou osobu;

2. „prostředkem pro elektronickou identifikaci“ hmotná či nehmotná jednotka obsahující data uvedená v bodě 1 tohoto článku, která se používají k přístupu k internetovým službám, jak je uvedeno v článku 5;

3. „systémem elektronické identifikace“ systém pro elektronickou identifikaci, na jehož základě jsou osobám uvedeným v bodě 1 tohoto článku vydávány prostředky pro elektronickou identifikaci;

4. „autentizací“ elektronický proces, který umožňuje ověřit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu elektronických dat;

5. „podepisující osobou“ fyzická osoba, která vytváří elektronický podpis;

6. „elektronickým podpisem“ údaje v elektronické podobě, které jsou připojeny k ostatním elektronickým datům nebo jsou s nimi logicky spojené a které podepisující osoba používá při podpisu;

7. „zaručeným elektronickým podpisem“ elektronický podpis, který splňuje tyto požadavky:

a) je jednoznačně spojen s podepisující osobou;

b) umožňuje identifikaci podepisující osoby;

c) je vytvořen pomocí dat pro vytváření elektronického podpisu, která může podepisující osoba s vysokou úrovní spolehlivosti použít pod svou výhradní kontrolou, a

d) je k datům, ke kterým se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat;

8. „kvalifikovaným elektronickým podpisem“ zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronického podpisu a který je založen na kvalifikovaném certifikátu pro elektronické podpisy;

9. „daty pro vytváření elektronického podpisu“ jedinečná data, která podepisující osoba používá k vytvoření elektronického podpisu;

10. „certifikátem“ elektronické potvrzení, které spojuje data pro ověřování elektronického podpisu nebo značky určité fyzické respektive právnické osoby s certifikátem a potvrzuje data této osoby;

11. „kvalifikovaným certifikátem pro elektronický podpis“ potvrzení, které se používá na podporu elektronických podpisů, je vydáno kvalifikovaným poskytovatelem důvěryhodných služeb a splňuje požadavky stanovené v příloze I;

12. „důvěryhodnou službou“ jakákoli elektronická služba spočívající ve vytváření, ověřování, potvrzování, zpracovávání a uchovávání elektronických podpisů, elektronických značek, elektronických časových razítek, elektronických dokumentů, elektronickém doručování, ověřování webových stránek a elektronických certifikátů, včetně certifikátů pro elektronické podpisy a pro elektronické značky;

13. „kvalifikovanou důvěryhodnou službou“ jakákoli důvěryhodná služba, která splňuje použitelné požadavky stanovené v tomto nařízení;

14. „poskytovatelem důvěryhodných služeb“ fyzická nebo právnická osoba, která poskytuje jednu či více důvěryhodných služeb;

15. „kvalifikovaným poskytovatelem důvěryhodných služeb“ poskytovatel důvěryhodných služeb, který splňuje požadavky stanovené v tomto nařízení;

16. „produktem“ technické zařízení nebo programové vybavení či jejich součásti, používané pro poskytování důvěryhodných služeb;

17. „prostředkem pro vytváření elektronického podpisu“ konfigurované programové vybavení nebo technické zařízení používané k vytvoření elektronického podpisu;

18. „kvalifikovaným prostředkem pro vytváření elektronického podpisu“ prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené v příloze II;

19. „označující osobou“ právnická osoba, která vytváří elektronickou značku;

20. „elektronickou značkou“ údaje v elektronické podobě, které jsou připojené k ostatním elektronickým datům nebo jsou s nimi logicky spojené s cílem zaručit původ a integritu připojených dat;

21. „zaručenou elektronickou značkou“ elektronická značka, která splňuje tyto požadavky:

a) je jednoznačně spojena s označující osobou;

b) umožňuje identifikaci označující osoby;

c) byla vytvořena pomocí dat pro vytváření elektronické značky, která může označující osoba s vysokou úrovní spolehlivosti použít k vytvoření elektronické značky pod svou kontrolou, a

d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možno zjistit jakoukoliv následnou změnu těchto dat;

22. „kvalifikovanou elektronickou značkou“ zaručená elektronická značka, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronické značky a která je založena na kvalifikovaném certifikátu pro elektronickou značku;

23. „daty pro vytváření elektronické značky“ jedinečná data, která označující osoba používá k vytvoření elektronické značky;

24. „kvalifikovaným certifikátem pro elektronickou značku“ potvrzení, které se používá na podporu elektronické značky, je vydáno kvalifikovaným poskytovatelem důvěryhodných služeb a splňuje požadavky stanovené v příloze III;

25. „elektronickým časovým razítkem“ údaje v elektronické podobě, které spojují ostatní elektronická data s časovým okamžikem a zaručují, že uvedená data existovala v daném časovém okamžiku;

26. „kvalifikovaným elektronickým časovým razítkem“ elektronické časové razítko, které splňuje požadavky stanovené v článku 33;

27. „elektronickým dokumentem“ dokument v elektronické podobě;

28. „elektronickým doručováním“ služba, která umožňuje přenášet data elektronickými prostředky a poskytuje důkazy týkající se zpracování přenášených dat, včetně dokladu o odeslání nebo přijetí dat, a která chrání přenášená data před rizikem ztráty, zcizení, poškození nebo neoprávněných změn;

29. „kvalifikovanou službou elektronického doručování“ elektronické doručování, které splňuje požadavky stanovené v článku 36;

30. „kvalifikovaným certifikátem pro ověřování webových stránek“ potvrzení, které umožňuje ověřit pravost webových stránek a spojuje webové stránky s osobou, jíž je vydán certifikát, který vydal kvalifikovaný poskytovatel důvěryhodných služeb a který splňuje požadavky stanovené v příloze IV;

31. „daty pro ověřování“ data, která se používají k ověření elektronického podpisu nebo elektronické značky.

Článek 4

Zásada vnitřního trhu

1. Nesmí existovat žádná omezení týkající se poskytování důvěryhodných služeb na území určitého členského státu poskytovatelem důvěryhodných služeb, který je usazen v jiném členském státě, z důvodů, jež spadají do oblastí, na něž se vztahuje toto nařízení.

2. Produkty, které vyhovují tomuto nařízení, se mohou volně pohybovat na vnitřním trhu.

KAPITOLA II

ELEKTRONICKÁ IDENTIFIKACE

Článek 5

Vzájemné uznávání a přijímání

Pokud se podle vnitrostátních právních předpisů nebo správní praxe pro přístup ke službě na internetu vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizace, je pro účely přístupu k této službě uznán a přijímán jakýkoli prostředek pro elektronickou identifikaci vydaný v jiném členském státě spadající do systému uvedeného v seznamu, který Komise zveřejní postupem podle článku 7.

Článek 6

Podmínky pro oznamování systémů elektronické identifikace

1. Systémy elektronické identifikace jsou způsobilé pro oznámení podle článku 7, jsou-li splněny všechny tyto podmínky:

a) prostředky pro elektronickou identifikaci jsou vydány oznamujícím členským státem, jeho jménem nebo v rámci jeho odpovědnosti;

b) prostředky pro elektronickou identifikaci lze použít pro přístup alespoň k veřejným službám, u nichž se v oznamujícím členském státě vyžaduje elektronická identifikace;

c) oznamující členský stát zajišťuje, že identifikační údaje osoby jsou jednoznačně spojeny s fyzickou nebo právnickou osobou uvedenou v čl. 3 bodě 1;

d) oznamující členský stát zajišťuje dostupnost možnosti autentizace na internetu, a to kdykoli a bezplatně, takže strana spoléhající se na autentizaci může ověřit platnost osobních identifikačních údajů, které obdržela v elektronické podobě. Členské státy nesmí spoléhajícím se stranám, které nejsou usazeny na jejich území a které chtějí provést takovouto autentizaci, ukládat zvláštní technické požadavky. Je-li narušena nebo částečně ohrožena bezpečnost oznámeného systému identifikace nebo možnosti autentizace, členské státy neprodleně pozastaví platnost oznámeného systému identifikace nebo možnosti autentizace či dotčených ohrožených součástí nebo je zruší a v souladu s článkem 7 vyrozumí ostatní členské státy a Komisi;

e) oznamující členský stát přebírá odpovědnost za:

– i) jednoznačné spojení osobních identifikačních údajů uvedených v písmenu c) a

– ii) možnost autentizace uvedenou v písmenu d).

2. Ustanovením v odst. 1 písm. e) není dotčena odpovědnost účastníků transakce, při níž jsou použity prostředky pro elektronickou identifikaci spadající do oznámeného systému.

Článek 7

Oznamování

1. Členské státy, které oznámí systémy elektronické identifikace, předají Komisi tyto informace a bezodkladně i jejich následné změny:

a) popis oznámeného systému elektronické identifikace;

b) orgány odpovědné za oznámený systém elektronické identifikace;

c) informace o tom, kdo spravuje evidenci jednoznačných osobních identifikačních údajů;

d) popis možnosti autentizace;

e) opatření k pozastavení platnosti nebo zrušení oznámeného systému identifikace nebo možnosti autentizace či ohrožených součástí.

2. Šest měsíců po vstupu nařízení v platnost zveřejní Komise v *Úředním věstníku Evropské unie* seznam systémů elektronické identifikace, které byly oznámeny podle odstavce 1, a základní informace o těchto systémech.

3. Obdrží-li Komise oznámení po uplynutí lhůty uvedené v odstavci 2, seznam pozmění do tří měsíců.

4. Komise může stanovit okolnosti, formáty a postupy oznamování uvedeného v odstavcích 1 a 3 prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 8

Koordinace

1. Členské státy vzájemně spolupracují v zájmu zajištění interoperability prostředků pro elektronickou identifikaci spadajících do oznámeného systému a zvýšení jejich bezpečnosti.

2. Komise stanoví potřebné podmínky pro usnadnění spolupráce mezi členskými státy uvedené v odstavci 1 v zájmu posílení vysoké úrovně důvěryhodnosti a bezpečnosti odpovídající míře rizika prostřednictvím prováděcích aktů. Tyto prováděcí akty se týkají zejména výměny informací, zkušeností a osvědčených postupů ohledně systémů elektronické identifikace, vzájemného hodnocení oznámených systémů elektronické identifikace a ověření příslušného vývoje v oblasti elektronické identifikace příslušnými orgány členských států. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

3. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o usnadnění přeshraniční interoperability prostředků pro elektronickou identifikaci, a to stanovením minimálních technických požadavků.

KAPITOLA III

DŮVĚRYHODNÉ SLUŽBY

Oddíl 1

Obecná ustanovení

Článek 9

Odpovědnost

1. Poskytovatel důvěryhodných služeb odpovídá za přímou škodu způsobenou fyzické nebo právnické osobě nesplněním povinností stanovených v čl. 15 odst. 1, ledaže poskytovatel důvěryhodné služby může prokázat, že nejednal z nedbalosti.

2. Kvalifikovaný poskytovatel důvěryhodných služeb odpovídá za přímou škodu způsobenou fyzické nebo právnické osobě nedodržením požadavků stanovených v tomto nařízení, zejména v článku 19, ledaže kvalifikovaný poskytovatel důvěryhodné služby může prokázat, že nejednal z nedbalosti.

Článek 10

Poskytovatelé důvěryhodných služeb ze třetích zemí

1. Kvalifikované důvěryhodné služby a kvalifikované certifikáty poskytované kvalifikovanými poskytovateli důvěryhodných služeb usazenými ve třetí zemi se přijímají jako kvalifikované důvěryhodné služby a kvalifikované certifikáty poskytované kvalifikovanými poskytovateli důvěryhodných služeb usazenými na území Unie, pokud jsou kvalifikované důvěryhodné služby nebo kvalifikované certifikáty pocházející ze třetí země uznány na základě dohody mezi Unií a třetími zeměmi nebo mezinárodními organizacemi v souladu s článkem 218 SFEU.

2. S odkazem na odstavec 1 tyto dohody zajistí, aby byly požadavky vztahující se na kvalifikované důvěryhodné služby a kvalifikované certifikáty poskytované kvalifikovanými poskytovateli důvěryhodných služeb usazenými na území Unie dodržovány poskytovateli důvěryhodných služeb ve třetích zemích nebo mezinárodními organizacemi, zejména co se týká ochrany osobních údajů, bezpečnosti a dohledu.

Článek 11

Zpracování a ochrana údajů

1. Při zpracovávání osobních údajů zajistí poskytovatelé důvěryhodných služeb a orgány dohledu korektní a zákonné zpracování v souladu se směrnicí 95/46/ES.

2. Poskytovatelé důvěryhodných služeb zpracovávají osobní údaje v souladu se směrnicí 95/46/ES. Toto zpracovávání je striktně omezeno na minimální údaje potřebné pro vydání a zachování certifikátu nebo poskytování důvěryhodných služeb.

3. Poskytovatelé důvěryhodných služeb zaručí důvěrnost a integritu údajů týkajících se osoby, které je poskytovaná důvěryhodná služba.

4. Aniž je dotčen právní účinek přiznaný pseudonymům podle vnitrostátního práva, nesmí členské státy bránit poskytovatelům důvěryhodných služeb v tom, aby v certifikátech pro elektronický podpis uváděly místo jména podepisující osoby pseudonym.

Článek 12

Přístupnost pro osoby se zdravotním postižením

Poskytované důvěryhodné služby a konečné uživatelské produkty používané při poskytování těchto služeb jsou pokud možno dostupné pro osoby se zdravotním postižením.

Oddíl 2

Dohled

Článek 13

Orgán dohledu

1. Členské státy určí vhodný orgán usazený na jejich území nebo po vzájemné dohodě v jiném členském státě v rámci odpovědnosti členského státu, který provedl určení. Orgánům dohledu jsou uděleny veškeré kontrolní a vyšetřovací pravomoci, které jsou nezbytné k plnění jejich úkolů.

2. Orgán dohledu odpovídá za plnění těchto úkolů:

a) sledování poskytovatelů důvěryhodných služeb usazených na území členského státu, který provedl určení, s cílem zajistit, aby plnili požadavky stanovené v článku 15;

b) provádění dohledu nad kvalifikovanými poskytovateli důvěryhodných služeb usazenými na území členského státu, který provedl určení, a poskytovanými kvalifikovanými důvěryhodnými službami s cílem zajistit, aby tito poskytovatelé a kvalifikované důvěryhodné služby, které poskytují, splňovali použitelné požadavky stanovené v tomto nařízení;

c) zajištění, aby příslušné informace a údaje uvedené v čl. 19 odst. 2 písm. g) a evidované kvalifikovanými poskytovateli důvěryhodných služeb byly za účelem zaručení kontinuity služby uchovávány po příslušnou dobu a byly k dispozici i po ukončení činnosti kvalifikovaného poskytovatele důvěryhodných služeb.

3. Každý orgán dohledu předloží Komisi a členským státům do konce prvního čtvrtletí následujícího roku výroční zprávu o činnosti v oblasti dohledu v minulém kalendářním roce. Tato zpráva obsahuje alespoň tyto údaje:

a) informace o činnosti v oblasti dohledu;

b) shrnutí oznámení o narušení bezpečnosti, která byla obdržena od poskytovatelů důvěryhodných služeb v souladu s čl. 15 odst. 2;

c) statistické údaje o trhu a o využívání kvalifikovaných důvěryhodných služeb, včetně informací o kvalifikovaných poskytovatelích důvěryhodných služeb, kvalifikovaných důvěryhodných službách, které poskytují, produktech, které používají, a obecného popisu jejich zákazníků.

4. Členské státy sdělí Komisi a ostatním členským státům názvy a adresy svých příslušných orgánů dohledu, které určily.

5. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o stanovení postupů vztahujících se na úkoly uvedené v odstavci 2.

6. Komise může stanovit okolnosti, formáty a postupy pro podávání zpráv podle odstavce 3 prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 14

Vzájemná pomoc

1. Orgány dohledu vzájemně spolupracují za účelem výměny osvědčených postupů a v nejkratší možné lhůtě si poskytují příslušné informace a vzájemnou pomoc, aby bylo možné zajistit jednotný výkon činnosti. Vzájemná pomoc se vztahuje zejména na žádosti o informace a opatření v oblasti dohledu, například žádosti o provedení prověrek v souvislosti s bezpečnostními audity, jak je uvedeno v článcích 15, 16 a 17.

2. Orgán dohledu, jemuž byla určena žádost o pomoc, jí musí vyhovět s výjimkou těchto případů:

a) orgán není pro vyřízení žádosti příslušný; nebo

b) vyhovění této žádosti by nebylo v souladu s tímto nařízením.

3. Orgány dohledu mohou případně provádět společná šetření, na nichž se podílejí pracovníci orgánů dohledu z ostatních členských států.

Orgán dohledu členského státu, v němž se má provést šetření, může v souladu se svými vnitrostátními právními předpisy svěřit vyšetřovací úkoly pracovníkům orgánu dohledu, kterému je poskytována pomoc. Tyto úkoly mohou být vykonávány pouze podle pokynů a v přítomnosti pracovníků z hostitelského orgánu dohledu. Pracovníci orgánu dohledu, kterému je poskytována pomoc, podléhají vnitrostátním právním předpisům hostitelského orgánu dohledu. Hostitelský orgán dohledu přebírá odpovědnost za činnost pracovníků orgánu dohledu, kterému je poskytována pomoc.

4. Komise může stanovit formáty a postupy pro vzájemnou pomoc stanovenou v tomto článku prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 15

Bezpečnostní požadavky vztahující se na poskytovatele důvěryhodných služeb

1. Poskytovatelé důvěryhodných služeb, kteří jsou usazeni na území Unie, přijmou odpovídající technická a organizační opatření za účelem řízení rizik ohrožujících bezpečnost důvěryhodných služeb, které poskytují. S ohledem na stav techniky tato opatření zajišťují úroveň bezpečnosti, která odpovídá míře rizika. Opatření jsou přijímána zejména s cílem zabránit bezpečnostním incidentům a omezit jejich dopady na nejnižší možnou úroveň a informovat zúčastněné strany o negativních dopadech těchto incidentů.

Aniž je dotčen čl. 16 odst. 1, může poskytovatel důvěryhodných služeb předložit orgánu dohledu zprávu o bezpečnostním auditu, který provedl uznaný nezávislý subjekt, za účelem potvrzení přijetí odpovídajících bezpečnostních opatření.

2. Poskytovatelé důvěryhodných služeb oznámí příslušnému orgánu dohledu, příslušnému vnitrostátnímu orgánu pro bezpečnost informací a ostatním příslušným třetím stranám, například orgánům pro ochranu údajů, případné narušení bezpečnosti nebo ztrátu integrity, jež mají významný dopad na poskytovanou důvěryhodnou službu a uchovávané osobní údaje, a to bez zbytečného odkladu, a je-li to možné, nejpozději do 24 hodin od chvíle, kdy toto narušení zjistili.

Je-li to vhodné, zejména v případě, týká-li se narušení bezpečnosti nebo ztráta integrity dvou nebo více členských států, informuje dotčený orgán dohledu orgány dohledu v ostatních členských státech a Evropskou agenturu pro bezpečnost sítí a informací (ENISA).

Dotčený orgán dohledu může informovat rovněž veřejnost nebo požádat, aby tak učinil poskytovatel důvěryhodné služby, pokud rozhodne, že zveřejnění informací o narušení bezpečnosti je ve veřejném zájmu.

3. Orgán dohledu poskytne ENISA a Komisi jednou ročně shrnutí oznámení o narušení bezpečnosti, která obdržel od poskytovatelů důvěryhodných služeb.

4. Za účelem provádění odstavců 1 a 2 je orgán dohledu zmocněn vydávat závazné pokyny pro poskytovatele důvěryhodných služeb.

5. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o upřesnění opatření uvedených v odstavci 1.

6. Komise může stanovit okolnosti, formáty a postupy, včetně lhůt, použitelné pro účely odstavců 1 až 3 prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 16

Dohled nad kvalifikovanými poskytovateli důvěryhodných služeb

1. Kvalifikovaní poskytovatelé důvěryhodných služeb jsou jednou ročně podrobeni auditu ze strany uznaného nezávislého subjektu za účelem potvrzení, že oni sami i kvalifikované důvěryhodné služby, které poskytují, splňují požadavky stanovené v tomto nařízení, a výslednou zprávu o bezpečnostním auditu předloží orgánu dohledu.

2. Aniž je dotčen odstavec 1, může orgán dohledu u kvalifikovaných poskytovatelů důvěryhodných služeb kdykoli provést kontrolu za účelem potvrzení, že oni sami i kvalifikované důvěryhodné služby, které poskytují, nadále splňují podmínky stanovené v tomto nařízení, a to z vlastního podnětu, nebo na žádost Komise. Pokud se zdá, že došlo k porušení pravidel týkajících se ochrany osobních údajů, sdělí orgán dohledu výsledky svých auditů orgánům pro ochranu údajů.

3. Orgán dohledu je zmocněn vydávat pro kvalifikované poskytovatele důvěryhodných služeb závazné pokyny k nápravě případného neplnění požadavků, jež bylo uvedeno ve zprávě o bezpečnostním auditu.

4. S odkazem na odstavec 3 ztratí kvalifikovaný poskytovatel důvěryhodných služeb v případě, že ve lhůtě stanovené orgánem dohledu nenapraví neplnění požadavků, status kvalifikovaného poskytovatele a orgán dohledu jej informuje o tom, že se jeho status odpovídajícím způsobem změní v důvěryhodných seznamech uvedených v článku 18.

5. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde u upřesnění podmínek, za nichž se uznává nezávislý subjekt provádějící audit uvedený v odstavci 1 tohoto článku a v čl. 15 odst. 1 a čl. 17 odst. 1.

6. Komise může stanovit okolnosti, postupy a formáty použitelné pro účely odstavců 1, 2 a 4 prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 17

Zahájení poskytování kvalifikované důvěryhodné služby

1. Kvalifikovaní poskytovatelé důvěryhodných služeb oznámí orgánu dohledu svůj záměr zahájit poskytování kvalifikované důvěryhodné služby a předloží orgánu dohledu zprávu o bezpečnostním auditu, který provedl uznaný nezávislý subjekt, jak je stanoveno v čl. 16 odst. 1. Kvalifikovaní poskytovatelé důvěryhodných služeb mohou zahájit poskytování kvalifikované důvěryhodné služby poté, co orgánu dohledu předložili oznámení a zprávu o bezpečnostním auditu.

2. Po předložení příslušných dokumentů orgánu dohledu podle odstavce 1 jsou kvalifikovaní poskytovatelé důvěryhodných služeb zařazeni na důvěryhodné seznamy uvedené v článku 18, které udávají, že bylo podáno oznámení.

3. Orgán dohledu ověří, zda kvalifikovaný poskytovatel důvěryhodných služeb a kvalifikované důvěryhodné služby, které poskytuje, splňují požadavky nařízení.

Orgán dohledu uvede stav kvalifikace kvalifikovaných poskytovatelů služeb a kvalifikovaných důvěryhodných služeb, které poskytují, v důvěryhodných seznamech po kladném závěru ověření, a to nejpozději do jednoho měsíce od oznámení podle odstavce 1.

Není-li ověření dokončeno do jednoho měsíce, vyrozumí orgán dohledu kvalifikovaného poskytovatele důvěryhodných služeb a uvede důvody prodlevy a lhůtu pro dokončení ověřování.

4. Kvalifikovaná důvěryhodná služba, která byla předmětem oznámení podle odstavce 1, nemůže být s ohledem na splnění správního postupu nebo formality dotčeným subjektem z veřejného sektoru odmítnuta kvůli tomu, že není zařazena na seznamy uvedené v odstavci 3.

5. Komise může stanovit okolnosti, formáty a postupy pro účely odstavců 1, 2 a 3 prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 18

Důvěryhodné seznamy

1. Každý členský stát vyhotoví, spravuje a zveřejňuje důvěryhodné seznamy s informacemi týkajícími se kvalifikovaných poskytovatelů důvěryhodných služeb, pro něž je příslušný, spolu s informacemi o poskytovaných kvalifikovaných důvěryhodných službách.

2. Členské státy vyhotoví, spravují a bezpečným způsobem zveřejní důvěryhodné seznamy uvedené v odstavci 1, které jsou opatřeny elektronickým podpisem nebo elektronickou značkou, a to ve formě vhodné pro automatické zpracování.

3. Členské státy bezodkladně sdělí Komisi informace o subjektu odpovědném za vyhotovení, vedení a zveřejnění vnitrostátních důvěryhodných seznamů a poskytnou informace o místě zveřejnění těchto seznamů, certifikátech použitých k opatření důvěryhodných seznamů elektronickým podpisem nebo značkou a o jejich případných změnách.

4. Prostřednictvím bezpečného kanálu zpřístupní Komise informace uvedené v odstavci 3 veřejnosti ve formě opatřené elektronickým podpisem nebo značkou, která je vhodná pro automatické zpracování.

5. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o vymezení informací uvedených v odstavci 1.

6. Komise může stanovit technické specifikace a formáty pro důvěryhodné seznamy, které jsou použitelné pro účely odstavců 1 až 4, prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 19

Požadavky na kvalifikované poskytovatele důvěryhodných služeb

1. Při vydávání kvalifikovaného certifikátu kvalifikovaný poskytovatel důvěryhodných služeb pomocí vhodných prostředků a v souladu s vnitrostátními právními předpisy ověří identitu a případně zvláštní znaky fyzické nebo právnické osoby, jíž je kvalifikovaný certifikát vydáván.

Tyto informace ověřuje kvalifikovaný poskytovatel služeb nebo zplnomocněná třetí osoba, která jedná v rámci odpovědnosti kvalifikovaného poskytovatele služeb, a to:

a) prostřednictvím fyzické identity fyzické osoby nebo zplnomocněného zástupce právnické osoby, nebo

b) na dálku s využitím prostředku pro elektronickou identifikaci v rámci oznámeného systému, který byl vydán v souladu s písmenem a).

2. Kvalifikovaní poskytovatelé důvěryhodných služeb poskytující kvalifikované důvěryhodné služby:

a) zaměstnávají pracovníky, kteří mají potřebné odborné znalosti, zkušenosti a kvalifikace a používají správní a řídicí postupy, které odpovídají evropským nebo mezinárodním normám, a absolvovali odpovídající odbornou přípravu týkající se bezpečnosti a pravidel ochrany osobních údajů;

b) nesou odpovědnost za škody a za tímto účelem udržují dostatečné finanční prostředky nebo uzavřeli pojištění odpovědnosti;

c) před uzavřením smluvního vztahu informují osobu, která chce využít kvalifikovanou důvěryhodnou službu, o přesných podmínkách používání této služby;

d) používají důvěryhodné systémy a produkty, které jsou chráněny proti pozměňování a které zajišťují technickou bezpečnost a spolehlivost procesu, který podporují;

e) používají důvěryhodné systémy k uchovávání údajů, které jsou jim poskytovány, v ověřitelné podobě, aby:

– byly veřejně přístupné pro účely vyhledávání pouze se souhlasem osoby, jíž byly údaje vydány,

– záznamy a změny mohly provádět pouze zmocněné osoby,

– bylo možno ověřit pravost informací;

f) přijímají opatření proti padělání a zcizení údajů;

g) po příslušnou dobu evidují veškeré příslušné informace týkající se dat, která vydal a obdržel kvalifikovaný poskytovatel důvěryhodných služeb, zejména pro účely poskytnutí důkazů v soudním řízení. Tato evidence může mít elektronickou podobu;

h) mají k dispozici aktualizovaný plán ukončení činnosti k zajištění kontinuity služby v souladu s rozhodnutími vydanými orgánem dohledu podle čl. 13 odst. 2 písm. c);

i) zajišťují zákonné zpracovávání osobních údajů v souladu s článkem 11.

3. Kvalifikovaní poskytovatelé důvěryhodných služeb vydávající kvalifikované certifikáty zaevidují ve své databázi certifikátů zrušení certifikátu do deseti minut poté, co nabylo účinnosti.

4. S odkazem na odstavec 3 poskytnou kvalifikovaní poskytovatelé důvěryhodných služeb vydávající kvalifikované certifikáty kterékoli spoléhající se straně informace o platnosti nebo o zrušení kvalifikovaných certifikátů, které vydali. Tyto informace jsou zpřístupněny kdykoli alespoň na základě certifikátu a automatickým způsobem, který je spolehlivý, bezplatný a účinný.

5. Komise může určit referenční čísla norem pro důvěryhodné systémy a produkty prostřednictvím prováděcích aktů. Pokud důvěryhodné systémy a produkty vyhovují těmto normám, předpokládá se shoda s požadavky stanovenými v článku 19. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Oddíl 3

Elektronický podpis

Článek 20

Právní účinky a přijímání elektronických podpisů

1. Elektronickým podpisům nesmí být upírány právní účinky a nesmí být odmítány jako důkazy v soudním řízení pouze z toho důvodu, že mají elektronickou podobu.

2. Kvalifikovaný elektronický podpis má rovnocenný právní účinek jako vlastnoruční podpis.

3. Kvalifikované elektronické podpisy jsou uznávány a přijímány ve všech členských státech.

4. Vyžaduje-li se u elektronického podpisu nižší záruka bezpečnosti než kvalifikovaný elektronický podpis, zejména požaduje-li jej členský stát pro přístup k internetové službě poskytované subjektem z veřejného sektoru na základě náležitého posouzení rizik spojených s takovouto službou, jsou uznávány a přijímány všechny elektronické podpisy poskytující přinejmenším stejnou záruku bezpečnosti.

5. Členské státy nesmí v případě přeshraničního přístupu k internetové službě poskytované subjektem z veřejného sektoru vyžadovat elektronický podpis s vyšší zárukou bezpečnosti než kvalifikovaný elektronický podpis.

6. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o stanovení různých úrovní bezpečnosti elektronického podpisu uvedených v odstavci 4.

7. Komise může určit referenční čísla norem pro úrovně bezpečnosti elektronického podpisu prostřednictvím prováděcích aktů. Pokud elektronický podpis vyhovuje těmto normám, předpokládá se shoda s úrovní bezpečnosti stanovenou v aktu v přenesené pravomoci přijatém podle odstavce 6. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v Úředním věstníku Evropské unie.

Článek 21

Kvalifikované certifikáty pro elektronický podpis

1. Kvalifikované certifikáty pro elektronický podpis splňují požadavky stanovené v příloze I.

2. Kvalifikované certifikáty pro elektronický podpis nepodléhají žádným závazným požadavkům, které přesahují požadavky stanovené v příloze I.

3. Pokud byl kvalifikovaný certifikát pro elektronický podpis po počáteční aktivaci zrušen, ztrácí svou platnost a jeho status se nemůže v žádném případě změnit obnovením jeho platnosti.

4. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde u upřesnění požadavků stanovených v příloze I.

5. Komise může určit referenční čísla norem pro kvalifikované certifikáty pro elektronický podpis prostřednictvím prováděcích aktů. Pokud kvalifikovaný certifikát pro elektronický podpis vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze I. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Článek 22

Požadavky na kvalifikované prostředky pro vytváření elektronického podpisu

1. Kvalifikované prostředky pro vytváření elektronického podpisu splňují požadavky stanovené v příloze II.

2. Komise může určit referenční čísla norem pro kvalifikované prostředky pro vytváření elektronického podpisu prostřednictvím prováděcích aktů. Pokud kvalifikovaný prostředek pro vytváření elektronického podpisu vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze II. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Článek 23

Certifikace kvalifikovaných prostředků pro vytváření elektronického podpisu

1. Kvalifikované prostředky pro vytváření elektronického podpisu mohou být certifikovány příslušnými veřejnými nebo soukromými subjekty, které určily členské státy, pokud byly podrobeny postupu posouzení bezpečnosti, který byl proveden v souladu s jednou z norem pro posuzování bezpečnosti produktů informačních technologií uvedených v seznamu, který Komise vyhotovila prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným přestupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

2. Členské státy sdělí Komisi a ostatním členským státům názvy a adresy soukromých nebo veřejných subjektů, které určily podle odstavce 1.

3. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o stanovení zvláštních kritérií, která mají splňovat určené subjekty uvedené v odstavci 1.

Článek 24

Zveřejnění seznamu certifikovaných kvalifikovaných prostředků pro vytváření elektronického podpisu

1. Členské státy bezodkladně sdělí Komisi informace o kvalifikovaných prostředcích pro vytváření elektronického podpisu, které byly certifikovány subjekty uvedenými v článku 23. Neprodleně předají Komisi rovněž informace o prostředcích pro vytváření elektronického podpisu, které již nebudou certifikovány.

2. Na základě obdržených informací Komise vyhotoví, zveřejní a spravuje seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronického podpisu.

3. Komise může stanovit okolnosti, formáty a postupy použitelné pro účely odstavce 1 prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 25

Požadavky na ověřování kvalifikovaných elektronických podpisů

1. Kvalifikovaný elektronický podpis se považuje za platný, pokud lze s vysokou úrovní spolehlivosti zjistit, že v době podpisu:

a) byl certifikát, který podporuje podpis, kvalifikovaným certifikátem pro elektronický podpis, jenž splňuje ustanovení uvedená v příloze I;

b) požadovaný kvalifikovaný certifikát je pravý a platný;

c) data pro ověřování podpisu odpovídají datům poskytnutým spoléhající se straně;

d) spoléhající se straně je řádně poskytnut soubor dat jednoznačně označujících podepisující osobu;

e) pokud je použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;

f) elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronického podpisu;

g) nebyla ohrožena integrita podepsaných dat;

h) jsou splněny požadavky stanovené v čl. 3 bodě 7;

i) systém použitý k ověření podpisu poskytuje spoléhající se straně řádný výsledek postupu ověření a umožňuje jí zjistit jakékoli záležitosti, které jsou důležité pro bezpečnost.

2. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o upřesnění požadavků stanovených v odstavci 1.

3. Komise může určit referenční čísla norem pro ověřování kvalifikovaných elektronických podpisů prostřednictvím prováděcích aktů. Pokud ověřování kvalifikovaných elektronických podpisů vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Článek 26

Kvalifikovaná služba pro ověřování kvalifikovaných elektronických podpisů

1. Kvalifikovaná služba pro ověřování kvalifikovaných elektronických podpisů je poskytována kvalifikovaným poskytovatelem důvěryhodných služeb, který:

a) zajišťuje ověřování v souladu s čl. 25 odst. 1 a

b) umožňuje, aby spoléhající se strany obdržely výsledek postupu ověřování automatickým způsobem, který je spolehlivý, účinný a je opatřen zaručeným

elektronickým podpisem nebo zaručenou elektronickou značkou poskytovatele kvalifikované služby pro ověřování.

2. Komise může určit referenční čísla norem pro kvalifikovanou službu pro ověřování uvedenou v odstavci 1 prostřednictvím prováděcích aktů. Pokud služba pro ověřování kvalifikovaných elektronických podpisů vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odst. 1 písm. b). Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Článek 27

Uchovávání kvalifikovaných elektronických podpisů

1. Kvalifikovanou službu pro uchovávání elektronických podpisů poskytuje kvalifikovaný poskytovatel důvěryhodných služeb, který používá postupy a technologie, které jsou s to zajistit důvěryhodnost dat pro ověřování kvalifikovaných elektronických podpisů i po uplynutí doby technické platnosti.

2. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o upřesnění požadavků stanovených v odstavci 1.

3. Komise může určit referenční čísla norem pro uchovávání kvalifikovaných elektronických podpisů prostřednictvím prováděcích aktů. Pokud prostředky pro uchovávání kvalifikovaných elektronických podpisů vyhovují těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Oddíl 4

Elektronické značky

Článek 28

Právní účinky elektronické značky

1. Elektronickým značkám nesmí být upírány právní účinky a nesmí být odmítány jako důkazy v soudním řízení pouze z toho důvodu, že mají elektronickou podobu.

2. U kvalifikované elektronické značky platí právní domněnka zaručení původu a integrity dat, s nimiž je spojena.

3. Kvalifikovaná elektronická značka je uznávána a přijímána ve všech členských státech.

4. Vyžaduje-li se u elektronické značky nižší záruka bezpečnosti než kvalifikovaná elektronická značka, zejména vyžaduje-li ji členský stát pro přístup k internetové službě poskytované subjektem z veřejného sektoru na základě náležitého posouzení rizik spojených s takovouto službou, jsou přijímány všechny elektronické značky poskytující přinejmenším stejnou záruku bezpečnosti.

5. Členské státy nesmí pro přístup k internetové službě nabízené subjektem z veřejného sektoru vyžadovat elektronickou značku s vyšší zárukou bezpečnosti než kvalifikovaná elektronická značka.

6. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o stanovení různých úrovní záruky bezpečnosti elektronických značek, jak je uvedeno v odstavci 4.

7. Komise může určit referenční čísla norem pro úrovně záruky bezpečnosti elektronických značek prostřednictvím prováděcích aktů. Pokud elektronická značka vyhovuje těmto normám, předpokládá se shoda s úrovní záruky bezpečnosti stanovenou v aktu v přenesené pravomoci přijatém podle odstavce 6. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Článek 29

Požadavky na kvalifikované certifikáty pro elektronickou značku

1. Kvalifikované certifikáty pro elektronickou značku splňují požadavky stanovené v příloze III.

2. Kvalifikované certifikáty pro elektronickou značku nepodléhají žádným dodatečným závazným požadavkům, které přesahují požadavky stanovené v příloze III.

3. Pokud byl kvalifikovaný certifikát pro elektronickou značku po počáteční aktivaci zrušen, ztrácí svou platnost a jeho status se nemůže v žádném případě změnit obnovením jeho platnosti.

4. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o upřesnění požadavků stanovených v příloze III.

5. Komise může určit referenční čísla norem pro kvalifikované certifikáty pro elektronickou značku prostřednictvím prováděcích aktů. Pokud kvalifikovaný certifikát pro elektronickou značku vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze III. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Článek 30

Kvalifikované prostředky pro vytváření elektronické značky

1. Na kvalifikované prostředky pro vytváření elektronické značky se vztahuje přiměřeně článek 22.

2. Na certifikaci kvalifikovaných prostředků pro vytváření elektronické značky se vztahuje přiměřeně článek 23.

3. Na zveřejnění seznamu certifikovaných kvalifikovaných prostředků pro vytváření elektronické značky se vztahuje přiměřeně článek 24.

Článek 31

Ověřování a uchovávání kvalifikovaných elektronických značek

Na ověřování a uchovávání kvalifikovaných elektronických značek se vztahují přiměřeně články 25, 26 a 27.

Oddíl 5

Elektronické časové razítko

Článek 32

Právní účinek elektronických časových razítek

1. Elektronickému časovému razítku nesmí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním řízení pouze z toho důvodu, že má elektronickou podobu.

2. U kvalifikovaného elektronického časového razítka platí právní domněnka zaručení časového okamžiku, který udává, a integrity dat, s nimiž je tento časový okamžik spojen.

3. Kvalifikované elektronické časové razítko je uznáváno a přijímáno ve všech členských státech.

Článek 33

Požadavky na kvalifikovaná elektronická časová razítka

1. Kvalifikované elektronické časové razítko splňuje tyto požadavky:

a) je přesně spojeno s koordinovaným světovým časem (UTC) tak, aby byla vyloučena možnost nezjistitelné změny dat;

b) je založeno na zdroji přesného času;

c) je vydáno kvalifikovaným poskytovatelem důvěryhodných služeb;

d) je podepsáno s použitím zaručeného elektronického podpisu nebo zaručené elektronické značky kvalifikovaného poskytovatele důvěryhodné služby nebo pomocí rovnocenné metody.

2. Komise může určit referenční čísla norem pro přesné spojování času s daty a zdroj přesného času prostřednictvím prováděcích aktů. Pokud přesné spojování času s daty a zdroj přesného času vyhovují těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Oddíl 6

Elektronické dokumenty

Článek 34

Právní účinky a přijímání elektronických dokumentů

1. Elektronický dokument se považuje za rovnocenný dokumentu v papírové podobě a je přípustný jako důkaz v soudním řízení, pokud jde o záruku jeho pravosti a integrity.

2. U dokumentu opatřeného kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou značkou osoby, která je oprávněna k vydání příslušného dokumentu, platí právní domněnka jeho pravosti a integrity, pokud dokument neobsahuje dynamické prvky, které mohou dokument automaticky změnit.

3. Vyžaduje-li se při poskytování internetové služby nabízené subjektem z veřejného sektoru originální dokument nebo ověřená kopie, uznávají se v ostatních členských státech bez dodatečných požadavků alespoň elektronické dokumenty, které jsou vydány osobami oprávněnými k vydávání příslušných dokumentů a které se podle vnitrostátních právních předpisů členského státu původu považují za originály nebo ověřené kopie.

4. Komise může stanovit formáty elektronických podpisů a značek, které jsou přijímány, pokud členský stát požaduje pro poskytnutí internetové služby nabízené subjektem z veřejného sektoru dokument opatřený podpisem nebo značkou uvedený v odstavci 2, prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Oddíl 7

Kvalifikovaná služba elektronického doručování

Článek 35

Právní účinek elektronického doručování

1. Data odeslaná nebo obdržená prostřednictvím elektronického doručování jsou přípustná jako důkaz v soudním řízení, pokud jde o integritu dat a spolehlivost data a času odeslání nebo přijetí těchto dat určeným příjemcem.

2. U dat odeslaných nebo obdržených prostřednictvím kvalifikované služby elektronického doručování platí právní domněnka integrity dat a spolehlivosti data a času odeslání nebo obdržení těchto dat udaného kvalifikovanou službou elektronického doručování.

3. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o upřesnění mechanismů pro odesílání nebo přijímání dat prostřednictvím elektronického doručování, které se používají za účelem posílení interoperability mezi službami elektronického doručování.

Článek 36

Požadavky na kvalifikované služby elektronického doručování

1. Kvalifikované služby elektronického doručování splňují tyto požadavky:

a) musí být poskytovány jedním či více kvalifikovanými poskytovateli důvěryhodných služeb;

b) musí umožnit jednoznačnou identifikaci odesílatele a případně příjemce;

c) proces odesílání a přijímání dat musí být zabezpečen prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické značky kvalifikovaného poskytovatele důvěryhodných služeb tak, aby byla vyloučena možnost nezjistitelné změny dat;

d) odesílatel a příjemce dat musí být jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat;

e) datum odeslání, přijetí a případná změna data musí být označeny prostřednictvím kvalifikovaného elektronického časového razítka;

f) v případě přenosu dat mezi dvěma či více kvalifikovanými poskytovateli důvěryhodných služeb se požadavky uvedené v písmenech a) až e) vztahují na všechny kvalifikované poskytovatele důvěryhodných služeb.

2. Komise může určit referenční čísla norem pro postupy odesílání a přijímání dat prostřednictvím prováděcích aktů. Pokud postup odesílání a přijímání dat vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

Oddíl 8

Ověřování webových stránek

Článek 37

Požadavky na kvalifikované certifikáty pro ověřování webových stránek

1. Kvalifikované certifikáty pro ověřování webových stránek splňují požadavky stanovené v příloze IV.

2. Kvalifikované certifikáty pro ověřování webových stránek jsou uznávány a přijímány ve všech členských státech.

3. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 38, pokud jde o upřesnění požadavků stanovených v příloze IV.

4. Komise může určit referenční čísla norem pro kvalifikované certifikáty pro ověřování webových stránek prostřednictvím prováděcích aktů. Pokud kvalifikovaný certifikát pro ověřování webových stránek vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze IV. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2. Komise zveřejní tyto akty v *Úředním věstníku Evropské unie*.

KAPITOLA IV

AKTY V PŘENESENÉ PRAVOMOCI

Článek 38

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 8 odst. 3, čl. 13 odst. 5, čl. 15 odst. 5, čl. 16 odst. 5, čl. 18 odst. 5, čl. 20 odst. 6, čl. 21 odst. 4, čl. 23 odst. 3, čl. 25 odst. 2, čl. 27 odst. 2, čl. 28 odst. 6, čl. 29 odst. 4, čl. 30 odst. 2, článku 31, čl. 35 odst. 3 a čl. 37 odst. 3 je svěřena Komisi na dobu neurčitou ode dne vstupu tohoto nařízení v platnost.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 8 odst. 3, čl. 13 odst. 5, čl. 15 odst. 5, čl. 16 odst. 5, čl. 18 odst. 5, čl. 20 odst. 6, čl. 21 odst. 4, čl. 23 odst. 2, čl. 25 odst. 2, čl. 27 odst. 2, čl. 28 odst. 6, čl. 29 odst. 4, čl. 30 odst. 2, článku 31, čl. 35 odst. 3 a čl. 37 odst. 3 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku dnem následujícím po zveřejnění rozhodnutí v *Úředním věstníku Evropské unie* nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

5. Akt v přenesené pravomoci přijatý podle čl. 8 odst. 3, čl. 13 odst. 5, čl. 15 odst. 5, čl. 16 odst. 5, čl. 18 odst. 5, čl. 20 odst. 6, čl. 21 odst. 4, čl. 23 odst. 3, čl. 25 odst. 2, čl. 27 odst. 2, čl. 28 odst. 6, čl. 29 odst. 4, čl. 30 odst. 2, článku 31, čl. 35 odst. 3 a čl. 37 odst. 3 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

KAPITOLA V

PROVÁDĚCÍ AKTY

Článek 39

Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení č. 182/2011.

KAPITOLA VI

ZÁVĚREČNÁ USTANOVENÍ

Článek 40

Zpráva

Komise předkládá Evropskému parlamentu a Radě zprávy o uplatňování tohoto nařízení. První zprávu předloží nejpozději do čtyř let od vstupu tohoto nařízení v platnost. Každé čtyři roky pak podává následné zprávy.

Článek 41

Zrušení

1. Směrnice 1999/93/ES se zrušuje.

2. Odkazy na zrušenou směrnici se považují za odkazy na toto nařízení.

3. Prostředky pro bezpečné vytváření podpisu, jejichž shoda byla stanovena podle čl. 3 odst. 4 směrnice 1999/93/ES, se považují za kvalifikované prostředky pro vytváření podpisu podle tohoto nařízení.

4. Kvalifikovaná osvědčení vydaná podle směrnice 1999/93/ES se pokládají za kvalifikované certifikáty pro elektronické podpisy podle tohoto nařízení až do doby skončení jejich platnosti, nejdéle však pět let od vstupu tohoto nařízení v platnost.

Článek 42

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda	*předseda*

PŘÍLOHA I

Požadavky na kvalifikované certifikáty pro elektronické podpisy

Kvalifikované certifikáty pro elektronické podpisy obsahují:

a) označení, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis, a to alespoň ve formě vhodné pro automatické zpracování;

b) soubor dat jednoznačně označujících kvalifikovaného poskytovatele důvěryhodných služeb, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a

- v případě právnické osoby: názvu a registračního čísla uvedeného v úředních záznamech,
- v případě fyzické osoby: jména osoby;

c) soubor dat jednoznačně označujících podepisující osobu, jíž je certifikát vydán, včetně alespoň jména podepisující osoby nebo pseudonymu, který je jako takový označen;

d) data pro ověřování elektronického podpisu, která odpovídají datům pro vytváření elektronického podpisu;

e) označení začátku a konce doby platnosti certifikátu;

f) identifikační číslo certifikátu, které musí být jedinečné u daného kvalifikovaného poskytovatele důvěryhodných služeb;

g) zaručený elektronický podpis nebo zaručenou elektronickou značku kvalifikovaného poskytovatele důvěryhodných služeb, který certifikát vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát podporující zaručený elektronický podpis nebo zaručenou elektronickou značku podle písmena g);

i) údaj o umístění služeb pro ověření platnosti certifikátu, které lze využít k zjištění platnosti kvalifikovaného certifikátu;

j) pokud jsou data pro vytváření elektronického podpisu spojená s daty pro ověřování elektronického podpisu obsažena v kvalifikovaném prostředku pro vytváření elektronického podpisu, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

PŘÍLOHA II

Požadavky na kvalifikované prostředky pro vytváření podpisu

1. Kvalifikované prostředky pro vytváření elektronického podpisu vhodnými technickými prostředky a postupy přinejmenším zajistí, aby:

a) bylo zajištěno utajení dat pro vytváření elektronického podpisu, která byla použita při vytvoření elektronického podpisu;

b) se data pro vytváření elektronického podpisu použitá při vytvoření elektronického podpisu mohla vyskytnout pouze jednou;

c) bylo dostatečně zajištěno, že data pro vytváření elektronického podpisu použitá při vytvoření elektronického podpisu nelze odvodit a že elektronický podpis je dostupnými technickými prostředky chráněn proti padělání;

d) podepisující osoba měla možnost data pro vytváření elektronického podpisu použitá při vytvoření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou.

2. Kvalifikované prostředky pro vytváření elektronického podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním.

3. Data pro vytváření elektronického podpisu jménem podepisující osoby vytváří nebo spravuje kvalifikovaný poskytovatel důvěryhodné služby.

4. Kvalifikovaní poskytovatelé důvěryhodných služeb, kteří spravují data pro vytváření elektronického podpisu jménem podepisující osoby, mohou pro účely zálohování kopírovat data pro vytváření elektronického podpisu, jsou-li splněny tyto požadavky:

a) bezpečnost zkopírovaných souborů dat musí být na stejné úrovni jako u původních souborů dat;

b) počet zkopírovaných souborů dat nesmí přesáhnout minimum potřebné pro zajištění kontinuity služby.

PŘÍLOHA III

Požadavky na kvalifikované certifikáty pro elektronické značky

Kvalifikované certifikáty pro elektronické značky obsahují:

a) označení, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou značku, a to alespoň ve formě vhodné pro automatické zpracování;

b) soubor dat jednoznačně označujících kvalifikovaného poskytovatele důvěryhodných služeb, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a

- v případě právnické osoby: názvu a registračního čísla uvedeného v úředních záznamech,
- v případě fyzické osoby: jména osoby;

c) soubor dat jednoznačně označujících právnickou osobu, jíž je certifikát vydán, včetně alespoň názvu a registračního čísla uvedeného v úředních záznamech;

d) data pro ověřování elektronické značky, která odpovídají datům pro vytváření elektronické značky;

e) označení začátku a konce doby platnosti certifikátu;

f) identifikační číslo certifikátu, které musí být jedinečné u daného kvalifikovaného poskytovatele důvěryhodných služeb;

g) zaručený elektronický podpis nebo zaručenou elektronickou značku kvalifikovaného poskytovatele důvěryhodných služeb, který certifikát vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát podporující zaručený elektronický podpis nebo zaručenou elektronickou značku podle písmena g);

i) údaj o umístění služeb pro ověření platnosti certifikátu, které lze využít k zjištění platnosti kvalifikovaného certifikátu;

j) pokud jsou data pro vytváření elektronické značky spojená s daty pro ověřování elektronické značky obsažena v kvalifikovaném prostředku pro vytváření elektronické značky, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

PŘÍLOHA IV

Požadavky na kvalifikované certifikáty pro ověřování webových stránek

Kvalifikované certifikáty pro ověřování webových stránek obsahují:

a) označení, že se certifikát vydává jako kvalifikovaný certifikát pro ověřování webových stránek, alespoň ve formě vhodné pro automatické zpracování;

b) soubor dat jednoznačně označujících kvalifikovaného poskytovatele důvěryhodných služeb, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a

- v případě právnické osoby: názvu a registračního čísla uvedeného v úředních záznamech,
- v případě fyzické osoby: jména osoby;

c) soubor dat jednoznačně označujících právnickou osobu, jíž je certifikát vydán, včetně alespoň názvu a registračního čísla uvedeného v úředních záznamech;

d) údaje z adresy (včetně alespoň města a členského státu) právnické osoby, jíž je certifikát vydán, jak je uvedena v úředních záznamech;

e) název domény nebo domén, které provozuje právnická osoba, jíž je certifikát vydán;

f) označení začátku a konce doby platnosti certifikátu;

g) identifikační číslo certifikátu, které musí být jedinečné u daného kvalifikovaného poskytovatele důvěryhodných služeb;

h) zaručený elektronický podpis nebo zaručenou elektronickou značku kvalifikovaného poskytovatele důvěryhodných služeb, který certifikát vydává;

i) údaj o místu, kde je bezplatně k dispozici certifikát podporující zaručený elektronický podpis nebo zaručenou elektronickou značku podle písmena h);

j) údaj o umístění služeb pro ověření platnosti certifikátu, které lze využít k zjištění platnosti kvalifikovaného certifikátu.

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

Tento finanční výkaz obsahuje podrobné údaje o požadavcích, pokud jde o správní výdaje potřebné k provádění navrhovaného nařízení o *elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu*.

Na základě legislativního postupu a diskuse za účelem přijetí navrhovaného nařízení EP a Radou bude Komise potřebovat dvanáct pracovníků na plný pracovní úvazek pro navrhování souvisejících aktů v přenesené pravomoci a prováděcích aktů, zajištění dostupnosti organizačních a technických norem, zpracovávání informací oznámených členských států, zejména uchovávání informací týkajících se důvěryhodných seznamů, zajištění informovanosti zúčastněných stran (zejména občanů a malých a středních podniků) o výhodách používání elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb a účast na diskusích se třetími zeměmi za účelem zajištění interoperability elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb na celosvětové úrovni.

1.1. Název návrhu/podnětu

Návrh Komise na nařízení o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu

1.2. Příslušné oblasti politik podle členění ABM/ABB[25]

09 INFORMAČNÍ SPOLEČNOST

1.3. Povaha návrhu/podnětu

☐ Návrh/podnět se týká **nové akce**

☐ Návrh/podnět se týká **nové akce následující po pilotním projektu / přípravné akci**[26]

☐ Návrh/podnět se týká **prodloužení stávající akce**

☑ Návrh/podnět se týká **akce přesměrované na jinou akci**

1.4. Cíle

1.4.1. Víceleté strategické cíle Komise sledované návrhem/podnětem

Obecnými cíli návrhu jsou cíle všeobecných politik EU, jichž se návrh týká, jako je strategie EU 2020. Návrh má zajistit, aby se Evropa „přeměnila v inteligentní a udržitelnou ekonomiku podporující začlenění a vykazující vysokou úroveň zaměstnanosti, produktivity a sociální soudržnosti“.

---

25 ABM: řízení podle činností (Activity-Based Management) – ABB: sestavování rozpočtu podle činností (Activity-Based Budgeting).

26 Uvedené v čl. 49 odst. 6 písm. a) nebo b) finančního nařízení.

1.4.2. Specifické cíle a příslušné aktivity ABM/ABB

Zvýšení důvěryhodnosti celoevropských elektronických transakcí a zajištění přeshraničního právního uznávání elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb a rovněž vysoké úrovně ochrany údajů a posílení postavení uživatelů na jednotném trhu (viz Digitální agenda pro Evropu, klíčová opatření 3 a 16). Příslušné aktivity ABM/ABB 09 02 – Právní rámec pro Digitální agendu pro Evropu

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Stanovení jednoznačného právního prostředí pro elektronickou identifikaci, autentizaci, podpis a související důvěryhodné služby, jež zvýší pohodlí a důvěru uživatelů v digitální svět.

1.4.4. Ukazatele výsledků a dopadů

Upřesněte ukazatele, podle kterých je možno uskutečňování návrhu/podnětu sledovat.

1. Existence poskytovatelů elektronické identifikace, autentizace a podpisu a souvisejících důvěryhodných služeb, kteří vykonávají činnosti ve více členských státech EU 2. Míra, v jaké jsou prostředky interoperabilní (např. čtečky inteligentních karet) mezi odvětvími a zeměmi 3. Využívání elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb všemi kategoriemi obyvatel 4. Míra, v jaké jsou elektronická identifikace, autentizace, podpis a související důvěryhodné služby využívány konečnými uživateli u vnitrostátních transakcí a mezinárodních (přeshraničních) transakcí 5. Míra harmonizace právních předpisů členských států týkajících se elektronické identifikace, autentizace, podpisu a souvisejících důvěryhodných služeb 6. Systémy elektronické identifikace oznámené Komisi 7. Služby dostupné s využitím oznámených prostředků pro elektronickou identifikaci ve veřejném sektoru (elektronická veřejná správa, elektronické zdravotnictví, elektronická justice, elektronické zadávání veřejných zakázek) 8. Služby dostupné s využitím oznámených prostředků pro elektronickou identifikaci v soukromém sektoru (internetové bankovnictví, elektronický obchod, elektronické hry, přihlašování na webové stránky, bezpečnější internetové služby).

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu

Rozdílné provedení směrnice o elektronickém podpisu v jednotlivých členských státech kvůli různému výkladu směrnice ze strany členských států způsobuje

problémy s přeshraniční operabilitou, a vede tudíž k nejednotnému prostředí v EU a narušení vnitřního trhu. To je doprovázeno nedostatečnou důvěryhodností elektronických systémů, jež evropským občanům brání používat v digitálním světě stejný druh služeb jako v reálném světě.

1.5.2. Přidaná hodnota ze zapojení EU

Opatření na úrovni EU by ve srovnání s opatřeními jednotlivých členských států znamenalo jednoznačné přínosy. Zkušenosti ve skutečnosti ukazují, že vnitrostátní opatření nejenže nejsou dostatečná pro umožnění přeshraničních elektronických transakcí, nýbrž naopak vytvořila překážky interoperability elektronických podpisů v celé Evropě a že v současnosti mají stejný dopad na elektronickou identifikaci, elektronickou autentizaci a související důvěryhodné služby.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Návrh je založen na zkušenostech se směrnicí o elektronickém podpisu a vyskytujících se problémech kvůli nejednotnému provedení a uplatňování uvedené směrnice, což znemožnilo dosáhnout jejích cílů.

1.5.4. Provázanost a možná synergie s dalšími relevantními nástroji

Na směrnici o elektronickém podpisu se odkazuje v řadě jiných iniciativ EU, které byly zavedeny k odstranění problémů souvisejících s interoperabilitou a přeshraničním uznáváním a přijímáním u určitých druhů elektronických transakcí, jako je směrnice o službách, směrnice o zadávání veřejných zakázek, revidovaná směrnice o DPH (elektronická fakturace) nebo nařízení o evropské občanské iniciativě.

Navrhované nařízení mimoto poskytne právní rámec, který je přínosný pro široké využívání rozsáhlých pilotních projektů, které byly na úrovni EU zavedeny na podporu rozvoje interoperabilních a důvěryhodných prostředků elektronické komunikace (včetně SPOCS, podporujícího uplatňování směrnice o službách; STORK, podporujícího rozvoj a používání interoperabilních elektronických průkazů totožnosti; PEPPOL, podporujícího rozvoj a využívání interoperabilních řešení v oblasti elektronického zadávání veřejných zakázek; epSOS, podporujícího rozvoj a používání interoperabilních řešení v oblasti elektronického zdravotnictví; eCodex, podporujícího rozvoj a využívání interoperabilních řešení v oblasti elektronické justice).

1.6. Doba trvání akce a finanční dopad

☐ **Časově omezený** návrh/podnět

– ☐ Návrh/podnět s platností od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finanční dopad od RRRR do RRRR

☑ **Časově neomezený** návrh/podnět

1.7. Předpokládaný způsob řízení[27]

☑ **Přímé centralizované řízení** Komisí

☐ **Nepřímé centralizované řízení**, při kterém jsou úkoly plnění rozpočtu svěřeny:

– ☐ výkonným agenturám

– ☐ subjektům zřízeným Společenstvími[28]

– ☐ vnitrostátním veřejnoprávním subjektům / subjektům pověřeným výkonem veřejné služby

– ☐ osobám pověřeným prováděním zvláštních opatření podle hlavy V Smlouvy o Evropské unii a označeným v příslušném základním právním aktu ve smyslu článku 49 finančního nařízení

☐ **Sdílené řízení** s členskými státy

☐ **Decentralizované řízení** s třetími zeměmi

☐ **Společné řízení** s mezinárodními organizacemi ***(upřesněte)***

Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.

Poznámky

[//]

[27] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[28] Uvedené v článku 185 finančního nařízení.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

První hodnocení se uskuteční 4 roky od vstupu nařízení v platnost. Nařízení obsahuje výslovné ustanovení o podávání zpráv, na jehož základě bude Komise předkládat Evropskému parlamentu a Radě zprávy o jeho uplatňování. Následné zprávy budou poté předkládány každé čtyři roky. Použije se metodika Komise pro hodnocení. Zmíněná hodnocení se budou provádět za pomoci cílených studií o provádění předmětných právních nástrojů, pomoci dotazníků určených vnitrostátním orgánům a pomocí diskusí s odborníky, workshopů, průzkumů Eurobarometru atd.

2.2. Systém řízení a kontroly

2.2.1. Zjištěná rizika

Bylo provedeno posouzení dopadů, které je připojeno k návrhu nařízení. Nový právní nástroj zajistí vzájemné přeshraniční uznávání a přijímání elektronické identifikace, zlepší stávající rámec pro elektronické podpisy, posílí vnitrostátní dohled nad poskytovateli důvěryhodných služeb a přizná právní účinek souvisejícím důvěryhodným službám a zajistí jejich uznávání. Zavádí rovněž používání aktů v přenesené pravomoci a prováděcích aktů jako mechanismu pro zajištění pružnosti s ohledem na technologický rozvoj.

2.2.2. Předpokládané metody kontroly

Na dodatečné prostředky se budou vztahovat stávající metody kontroly, které Komise používá.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření.

Na dodatečné prostředky se budou vztahovat stávající opatření k zamezení podvodům, které Komise používá.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové linie

- Stávající výdajové rozpočtové linie

V pořadí okruhů víceletého finančního rámce a rozpočtových linií.

Okruh víceletého finančního rámce	Rozpočtová linie	Druh výdaje	Příspěvek			
	číslo [název……..……]	RP/NRP[29]	zemí ESVO[30]	kandidátských zemí[31]	třetích zemí	ve smyslu čl. 18 odst. 1 písm. aa) finančního nařízení
5	09. 01 01 01 Výdaje vztahující se k zaměstnancům v činné službě pracujícím v GŘ pro informační společnost a média	NRP	NE	NE	NE	NE
5	09. 01 02 01 Externí pracovníci	NRP	NE	NE	NE	NE

29 RP = rozlišené prostředky / NRP = nerozlišené prostředky.

30 ESVO: Evropské sdružení volného obchodu.

31 Kandidátské země a případně potenciální kandidátské země západního Balkánu.

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

Okruh víceletého finančního rámce:	Číslo	[Okruh 1. **Inteligentní růst podporující začlenění** ……..……]

GŘ: INFSO			Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok 2018	**Rok 2019**	**Rok 2020**	**CELKEM**
•Operační prostředky										
Číslo rozpočtové linie nevztahuje se na tento návrh	Závazky	(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 rozpočtové linie nevztahuje se na tento návrh	Závazky	(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**
Prostředky správní povahy financované z rámce na zvláštní programy[32]			0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Číslo rozpočtové linie		(3)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
CELKEM prostředky pro GŘ INFSO	Závazky	=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**

Okruh víceletého finančního rámce:	**5**	„Správní výdaje“

[32] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé linie „BA“), nepřímý výzkum, přímý výzkum.

v milionech EUR (zaokrouhleno na 3 desetinná místa)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**CELKEM**
		GŘ: INFSO							
• Lidské zdroje		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Ostatní správní výdaje									
GŘ INFSO **CELKEM**	Prostředky	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

CELKEM prostředky z OKRUHU 5 víceletého finančního rámce	(Závazky celkem = platby celkem)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

v milionech EUR (zaokrouhleno na 3 desetinná místa)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**CELKEM**
CELKEM prostředky z OKRUHU 1 až 5 víceletého finančního rámce	Závazky	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 dopad na operační prostředky

– ☑ Návrh/podnět nevyžaduje využití operačních prostředků

– ☐ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

3.2.3. Odhadovaný dopad na prostředky správní povahy

3.2.3.1. Shrnutí

– ☐ Návrh/podnět nevyžaduje využití správních prostředků

– ☑ Návrh/podnět vyžaduje využití správních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na 3 desetinná místa)

	Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**CELKEM**
OKRUH 5 víceletého finančního rámce								
Lidské zdroje	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Ostatní správní výdaje								
Mezisoučet za OKRUH 5 víceletého finančního rámce	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Mimo OKRUH 5[33] víceletého finančního rámce								
Lidské zdroje								
Ostatní výdaje správní povahy								
Mezisoučet mimo OKRUH 5 víceletého finančního rámce								

CELKEM	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé linie „BA“), nepřímý výzkum, přímý výzkum.

3.2.3.2. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů
– ☑ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v celých číslech (nebo zaokrouhlete nejvýše na 1 desetinné místo)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
09 01 01 01 (v ústředí a v zastoupeních Komise)		9	9	9	9	9	9	9
XX 01 01 02 (při delegacích)								
XX 01 05 01 (v nepřímém výzkumu)								
10 01 05 01 (v přímém výzkumu)								
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[34]								
09 01 02 01 (SZ, ZAP, VNO z celkového rámce)		3	3	3	3	3	3	3
XX 01 02 02 (SZ, ZAP, MOD, MZ a VNO při delegacích)								
XX 01 04 ***yy*** [35]	- v ústředí[36]							
	- při delegacích							
XX 01 05 02 (SZ, ZAP, VNO v nepřímém výzkumu)								
10 01 05 02 (SZ, ZAP, VNO v přímém výzkumu)								
Jiné rozpočtové linie (upřesněte)								
CELKEM		**12**	**12**	**12**	**12**	**12**	**12**	**12**

– Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	Řízení legislativních postupů pro přijetí plánovaného nařízení a souvisejících aktů v přenesené pravomoci / prováděcích aktů EP a Radou. Prioritní oblasti: 1. Zavedení nového právního rámce pro důvěryhodné elektronické služby 2. Podpora využívání důvěryhodných elektronických služeb zvýšením informovanosti malých a středních podniků o jejich potenciálu 3. Navázání na směrnici 1999/93/ES včetně mezinárodních aspektů 4. Využívání rozsáhlých pilotních projektů s cílem urychlit dosažení cíle nového legislativního rámce.
Externí zaměstnanci	Stejné jako výše

[34] SZ = smluvní zaměstnanec; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci; MZ = místní zaměstnanec; VNO = vyslaný národní odborník.

[35] Dílčí strop na externí pracovníky z operačních prostředků (bývalé linie „BA“).

[36] V podstatě na strukturální fondy, Evropský zemědělský fond pro rozvoj venkova (EZFRV) a Evropský rybářský fond.

3.2.4. Soulad se stávajícím víceletým finančním rámcem

– ☑ Návrh/podnět je v souladu se stávajícím víceletým finančním rámcem.

– ☐ Návrh/podnět si vyžádá úpravu příslušného okruhu víceletého finančního rámce.

Upřesněte požadovanou úpravu, příslušné rozpočtové linie a odpovídající částky.

– ☐ Návrh/podnět vyžaduje použití nástroje pružnosti nebo změnu víceletého finančního rámce[37].

Upřesněte potřebu, příslušné okruhy a rozpočtové linie a odpovídající částky.

3.2.5. Příspěvky třetích stran

– ☑ Návrh/podnět nepočítá se spolufinancováním od třetích stran

– ☐ Návrh/podnět počítá se spolufinancováním podle následujícího odhadu:

3.3. Odhadovaný dopad na příjmy

– ☑ Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☐ Návrh/podnět má tento finanční dopad:

- ☐ dopad na vlastní zdroje
- ☐ dopad na různé příjmy

[37] Viz body 19 a 24 interinstitucionální dohody.