NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014

ze dne 23. července 2014

o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

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 [1],

v souladu s řádným legislativním postupem [2],

vzhledem k těmto důvodům:

(1) Budování důvěryhodnosti on-line prostředí má pro hospodářský a sociální rozvoj klíčový význam. Nedostatečná důvěra, zejména v důsledku pocitu nedostatku právní jistoty, vede k tomu, že se spotřebitelé, podniky a orgány veřejné moci zdráhají provádět transakce elektronickými prostředky a přijímat nové služby.

(2) Toto nařízení má zvýšit důvěryhodnost elektronických transakcí na vnitřním trhu tím, že poskytne společný základ pro bezpečnou elektronickou komunikaci mezi občany, podniky, orgány veřejné moci, čímž posílí efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a elektronického obchodu v Unii.

(3) Směrnice Evropského parlamentu a Rady 1999/93/ES [3] upravovala elektronické podpisy, aniž by poskytovala ucelený přeshraniční a meziodvětvový rámec pro bezpečné, důvěryhodné a snadno použitelné elektronické transakce. Toto nařízení *acquis* uvedené směrnice posiluje a rozšiřuje.

(4) Ve sdělení Komise ze dne 26. srpna 2010 s názvem „Digitální agenda pro Evropu" byly jako hlavní překážky účinného cyklu digitální ekonomiky označeny roztříštěnost digitálního trhu, nedostatečná interoperabilita a nárůst kyberkriminality. Ve své zprávě o občanství EU za rok 2010 s názvem „Odstranit překážky pro výkon práv občanů EU" dále Komise vyzdvihla potřebu odstranit hlavní problémy, které občanům Unie brání ve využívání výhod jednotného digitálního trhu a přeshraničních digitálních služeb.

(5) Evropská rada ve svých závěrech ze dnů 4. února 2011 a 23. října 2011 vyzvala Komisi, aby do roku 2015 vytvořila jednotný digitální trh s cílem urychleně pokročit v klíčových oblastech digitálního hospodářství a aby prosazovala plně integrovaný jednotný digitální trh usnadněním přeshraničního využívání on-line služeb a zvláštní pozornost přitom věnovala usnadnění bezpečné elektronické identifikace a autentizace.

---

[1] Úř. věst. C 351, 15.11.2012, s. 73.

[2] Postoj Evropského parlamentu ze dne 3. dubna 2014 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 23. července 2014.

[3] Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (Úř. věst. L 13, 19.1.2000, s. 12).

(6) Rada ve svých závěrech ze dne 27. května 2011 Komisi vyzvala, aby přispěla k jednotnému digitálnímu trhu vytvořením vhodných podmínek pro vzájemné přeshraniční uznávání klíčových prvků, jako jsou elektronická identifikace, elektronické dokumenty, elektronické podpisy a služby elektronického doručování, a pro interoperabilní služby elektronické veřejné správy v celé Evropské unii.

(7) Evropský parlament ve svém usnesení ze dne 21. září 2010 o dotvoření vnitřního trhu pro elektronický obchod ([1]) 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.

(8) Směrnice Evropského parlamentu a Rady 2006/123/ES ([2]) 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 on-line služeb přístupných prostřednictvím jednotného kontaktního místa vyžaduje elektronickou identifikaci, autentizaci a podpis.

(9) Ve většině případů nemohou občané svou elektronickou identifikaci využívat k autentizaci v jiném členském státě, neboť vnitrostátní systémy elektronické identifikace v jejich zemi nejsou uznávány v ostatních členských státech. Tato elektronická bariéra znemožňuje poskytovatelům služeb plně využívat výhod vnitřního trhu. Vzájemně uznávané 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 moci potýkaly s mnoha překážkami.

(10) Směrnice Evropského parlamentu a Rady 2011/24/EU ([3]) zřídila síť vnitrostátních orgánů odpovědných za elektronické zdravotnictví. V zájmu zvýšení bezpečnosti a zajištění kontinuity přeshraniční zdravotní péče je tato síť povinna vypracovat pokyny k přeshraničnímu přístupu k elektronickým zdravotním údajům a službám, mimo jiné podporou „společných opatření pro identifikaci a ověřování za účelem snadnější přenositelnosti údajů v rámci přeshraniční zdravotní péče“. Vzájemné uznávání 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, musí být údaje o jejich zdravotním stavu dostupné v zemi, v níž je léčba poskytována. To vyžaduje řádný, bezpečný a důvěryhodný rámec pro elektronickou identifikaci.

(11) Toto nařízení by mělo být uplatňováno v plném souladu se zásadami ochrany osobních údajů podle směrnice Evropského parlamentu a Rady 95/46/ES ([4]). V tomto směru by se, s ohledem na zásadu vzájemného uznávání stanovenou v tomto nařízení, měla autentizace pro účely on-line služeb týkat zpracování pouze těch identifikačních údajů, které jsou přiměřené, podstatné a rozsahem úměrné pro udělení přístupu k dané on-line službě. Dále by poskytovatelé služeb vytvářejících důvěru a orgány dohledu měly dodržovat požadavky stanovené ve směrnici 95/46/ES týkající se důvěrné povahy a bezpečnosti zpracování.

(12) Jedním z cílů tohoto nařízení je odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají k autentizaci, alespoň pro účely veřejných služeb. Toto nařízení nemá za cíl zasahovat do systémů správy elektronické identity a souvisejících infrastruktur zřízených v členských státech. Jeho cílem je zajistit, aby u přístupu k přeshraničním on-line službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace.

([1]) Úř. věst. C 50 E, 21.2.2012, s. 1.
([2]) Směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu (Úř. věst. L 376, 27.12.2006, s. 36).
([3]) Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči (Úř. věst. L 88, 4.4.2011, s. 45).
([4]) Směrnice 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 (Úř. věst. L 281, 23.11.1995, s. 31).

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

(14) V tomto nařízení je nutno stanovit určité podmínky, pokud jde o to, které prostředky pro elektronickou identifikaci musí být uznávány, a způsob oznamování systémů elektronické identifikace. Tyto podmínky by měly členským státům pomoci při budování nezbytné vzájemné důvěry v systémy elektronické identifikace a při vzájemném uznávání prostředků pro elektronickou identifikaci spadajících do jejich oznámených systémů. Zásada vzájemného uznávání by se měla použít, jestliže systém elektronické identifikace oznamujícího členského státu splňuje podmínky pro oznámení a toto oznámení bylo zveřejněno v *Úředním věstníku Evropské unie*. Zásada vzájemného uznávání by se však měla týkat pouze autentizace pro účely on-line služby. Přístup k těmto on-line službám a jejich skutečné poskytnutí žadateli by měly úzce souviset s právem na obdržení takovýchto služeb za podmínek stanovených ve vnitrostátních právních předpisech.

(15) Povinnost uznávat prostředky pro elektronickou identifikaci by se měla týkat pouze těch prostředků, jejichž úroveň záruky totožnosti odpovídá úrovni, která je stejná nebo vyšší než úroveň požadovaná pro dotyčnou on-line službu. Kromě toho by tato povinnost měla platit pouze v případě, že dotyčný subjekt veřejného sektoru používá v souvislosti s přístupem k dané on-line službě značnou nebo vysokou úroveň záruky. Členské státy by měly mít možnost uznávat v souladu s právem Unie prostředky pro elektronickou identifikaci, které mají nižší úrovně záruky totožnosti.

(16) Úrovně záruky by měly vyjadřovat míru spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti osob, a tím poskytovat záruku, že osoba deklarující konkrétní totožnost je skutečně osobou, s níž je tato totožnost spojena. Úroveň záruky závisí na míře spolehlivosti, kterou daný prostředek pro elektronickou identifikaci u deklarované nebo uváděné totožnosti osoby poskytuje s přihlédnutím k postupům (například prokazování a ověřování totožnosti a autentizace), řídícím činnostem (například subjekt vydávající prostředky pro elektronickou identifikaci a postup vydávání těchto prostředků) a prováděným technickým kontrolám. V důsledku rozsáhlých pilotních projektů financovaných Unií, normalizace a činností v mezinárodním měřítku existují různé technické definice a popisy úrovní záruk. Zejména rozsáhlý pilotní projekt STORK a norma ISO 29115 uvádějí mimo jiné úrovně 2, 3 a 4, které by měly být v maximální míře zohledněny při stanovování minimálních technických požadavků, norem a postupů pro nízkou, značnou a vysokou úroveň záruky ve smyslu tohoto nařízení, a současně by mělo být zajištěno jednotné uplatňování tohoto nařízení, zejména pokud jde o vysokou úroveň záruky v souvislosti s prokazováním totožnosti pro vydávání kvalifikovaných certifikátů. Stanovené požadavky by měly být z technologického hlediska neutrální. Měla by tedy existovat možnost splnit nezbytné bezpečnostní požadavky různými technologiemi.

(17) Členské státy by měly podporovat soukromý sektor, aby pro účely identifikace, je-li u on-line služeb nebo elektronických transakcí zapotřebí, dobrovolně používal prostředky pro elektronickou identifikaci v rámci oznámeného systému. 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 k on-line službám. V zájmu snazšího přeshraničního používání těchto prostředků pro elektronickou identifikaci soukromým sektorem by možnost autentizace zajišťovaná kterýmkoli členským státem měla být k dispozici i spoléhajícím se stranám ze soukromého sektoru, které jsou usazeny mimo území daného členského státu, a to za stejných podmínek jako pro spoléhající se strany ze soukromého sektoru, které v daném členském státě usazeny jsou. Oznamující členský stát tak může stanovit podmínky přístupu spoléhajících se stran ze soukromého sektoru k prostředkům pro autentizaci. Tyto podmínky přístupu mohou informovat o tom, zda je prostředek pro autentizaci související s oznámeným systémem v současnosti dostupný spoléhajícím se stranám ze soukromého sektoru.

(18) Toto nařízení by mělo stanovit odpovědnost oznamujícího členského státu, strany vydávající prostředky pro elektronickou identifikaci a strany provozující postup autentizace za nedodržení příslušných povinností z tohoto nařízení vyplývajících. Mělo by však být uplatňováno v souladu s vnitrostátními pravidly odpovědnosti. Tato vnitrostátní pravidla týkající se například vymezení škod nebo souvisejících platných procesních pravidel, včetně důkazního břemene, jím proto nejsou dotčena.

(19) Bezpečnost systémů elektronické identifikace je klíčovým předpokladem pro důvěryhodné přeshraniční vzájemné uznávání prostředků pro elektronickou identifikaci. Členské státy by v této souvislosti měly spolupracovat v otázkách bezpečnosti a interoperability systémů elektronické identifikace na úrovni Unie. Ve všech případech, kdy systémy elektronické identifikace vyžadují, aby spoléhající se strany použily na vnitrostátní úrovni zvláštní technické zařízení nebo programové vybavení, je v zájmu přeshraniční interoperability žádoucí, aby tyto členské státy takové požadavky a související náklady neuplatňovaly vůči spoléhajícím se stranám usazeným mimo jejich území. V takovém případě je v mezích rámce interoperability třeba projednat a vyvinout vhodná řešení. Nicméně technické požadavky, které vyplývají z vlastních specifikací vnitrostátních prostředků pro elektronickou identifikaci a mohou mít vliv na držitele těchto elektronických prostředků (například inteligentní karty), jsou nevyhnutelné.

(20) Spolupráce členských států by měla usnadnit technickou interoperabilitu oznámených systémů elektronické identifikace v zájmu podpory 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.

(21) Toto nařízení by mělo stanovit rovněž obecný právní rámec pro využívání služeb vytvářejících důvěru. Nemělo by však zakládat obecnou povinnost používat tyto služby ani zřídit přístupový bod pro všechny existující služby vytvářející důvěru. Zejména by se nemělo vztahovat na poskytování služeb, které jsou využívány výhradně uvnitř uzavřených systémů mezi určeným okruhem účastníků a nemají žádný vliv na třetí osoby. Požadavky tohoto nařízení by se neměly například vztahovat na systémy zavedené v podnicích nebo v orgánech veřejné správy za účelem řízení vnitřních postupů využívajících služby vytvářející důvěru. Měly by jim podléhat pouze služby vytvářející důvěru, které jsou poskytovány veřejnosti a které mají vliv na třetí osoby. Toto nařízení by se nemělo vztahovat ani na aspekty související s uzavíráním a platností smluv nebo jiných právních povinností, pokud existují požadavky na formu stanovené vnitrostátním právem nebo právem Unie. Neměly by jím být dotčeny ani vnitrostátní požadavky na formu týkající se veřejných rejstříků, zejména obchodních rejstříků a katastrů nemovitostí.

(22) Aby se přispělo k obecnému přeshraničnímu využívání služeb vytvářejících důvěru, mělo by být možné použít je ve všech členských státech jako důkaz v soudním a správním řízení. Je na vnitrostátním právu, aby vymezilo právní účinky služeb vytvářejících důvěru, nestanoví-li se v tomto nařízení jinak.

(23) Pokud toto nařízení ukládá povinnost uznávat určitou službu vytvářející důvěru, může být její uznání odmítnuto pouze v případě, že ji povinný subjekt z technických důvodů, které jsou mimo jeho přímou kontrolu, není schopen přečíst nebo ověřit. Tato povinnost by však sama o sobě neměla znamenat, že veřejný subjekt musí získat technické zařízení a programové vybavení nezbytné pro technickou čitelnost všech existujících služeb vytvářejících důvěru.

(24) Členské státy mohou v souladu s právem Unie zachovat nebo zavést vnitrostátní předpisy týkající se služeb vytvářejících důvěru, pokud dané služby nejsou tímto nařízením plně harmonizovány. Služby vytvářející důvěru, které vyhovují tomuto nařízení, by se však měly na vnitřním trhu volně pohybovat.

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

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

(27) 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.

(28) Ke zvýšení důvěry zejména malých a středních podniků a spotřebitelů ve vnitřní trh a na podporu používání služeb vytvářejících důvěru a produktů by měly být zavedeny pojmy „kvalifikované služby vytvářející důvěru“ a „kvalifikovaný poskytovatel služeb vytvářejících důvěru“ za účelem stanovení požadavků a povinností, které zajistí vysokou úroveň bezpečnosti všech používaných nebo poskytovaných kvalifikovaných služeb vytvářejících důvěru a produktů.

(29) V souladu se závazky podle Úmluvy OSN o právech osob se zdravotním postižením, která byla schválena rozhodnutím Rady 2010/48/ES ([1]), a zejména s jejím článkem 9, by osoby se zdravotním postižením měly mít možnost využívat služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb stejně jako ostatní spotřebitelé. Poskytované služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb by proto měly být dostupné osobám se zdravotním postižením, je-li to proveditelné. Součástí posouzení proveditelnosti by měly být mimo jiné technické a ekonomické aspekty.

(30) Členské státy by měly určit orgán nebo orgány dohledu, které budou vykonávat činnosti v oblasti dohledu podle tohoto nařízení. Na základě vzájemné dohody s jiným členským státem by členské státy rovněž měly mít možnost rozhodnout, že určí orgán dohledu na území tohoto jiného členského státu.

(31) Orgány dohledu by měly spolupracovat s orgány pro ochranu údajů, například je informovat o výsledcích auditů kvalifikovaných poskytovatelů služeb vytvářejících důvěru, jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů. Toto poskytování informací by se mělo týkat zejména bezpečnostních incidentů a narušení bezpečnosti osobních údajů.

(32) Všichni poskytovatelé služeb vytvářejících důvěru by měli mít povinnost uplatňovat řádné bezpečnostní postupy, které jsou přiměřené s ohledem na rizika spojená s jejich činnostmi, aby byla posílena důvěra uživatelů v jednotný trh.

(33) Ustanovení o používání pseudonymů v certifikátech by neměla členským státům bránit v tom, aby vyžadovaly identifikaci osob podle práva Unie nebo podle vnitrostátního práva.

(34) Všechny členské státy by měly dodržovat společné základní požadavky na dohled s cílem zajistit srovnatelnou úroveň bezpečnosti kvalifikovaných služeb vytvářejících důvěru. 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.

(35) Požadavky tohoto nařízení, zejména požadavky týkající se bezpečnosti a povinnosti zajistit hloubkovou kontrolu operací a služeb, jejich transparentnost a odpovědnost za ně, by se měly vztahovat na všechny poskytovatele služeb vytvářejících důvěru. S přihlédnutím k druhu služeb, které poskytovatelé služeb vytvářejících důvěru poskytují, je však vhodné rozlišovat v souvislosti s těmito požadavky kvalifikované a nekvalifikované poskytovatele služeb vytvářejících důvěru.

(36) Zavedení režimu dohledu pro všechny poskytovatele služeb vytvářejících důvěru by zajistilo rovné podmínky pro bezpečnost jejich činností a služeb a odpovědnost za ně, což by přispělo k ochraně uživatelů a k fungování vnitřního trhu. Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru by měli podléhat nezatěžujícím a pružným činnostem následného dohledu, odůvodněným povahou jejich služeb a činností. Orgán dohledu by proto neměl mít obecnou povinnost vykonávat nad nekvalifikovanými poskytovateli služeb dohled. Orgán dohledu by měl jednat pouze v případě, že byl (například samotným nekvalifikovaným poskytovatelem služeb vytvářejících důvěru, jiným orgánem dohledu, na základě oznámení uživatele či obchodního partnera nebo na základě vlastního šetření) informován o tom, že nekvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje požadavky tohoto nařízení.

([1]) Rozhodnutí Rady 2010/48/ES ze dne 26. listopadu 2009 o uzavření Úmluvy Organizace spojených národů o právech osob se zdravotním postižením Evropským společenstvím (Úř. věst. L 23, 27.1.2010, s. 35).

(37) Toto nařízení by mělo stanovit odpovědnost pro všechny poskytovatele služeb vytvářejících důvěru. Zejména zavádí režim odpovědnosti, podle kterého by všichni poskytovatelé služeb vytvářejících důvěru měli odpovídat za škodu, kterou fyzické nebo právnické osobě způsobí v důsledku nesplnění povinností podle tohoto nařízení. Za účelem snadnějšího posouzení finančního rizika, které poskytovatelé služeb vytvářejících důvěru mohou být nuceni nést nebo které by mělo být kryto jejich pojistnou smlouvou, toto nařízení poskytovatelům služeb vytvářejících důvěru umožňuje stanovit za určitých podmínek omezení týkající se využívání jimi poskytovaných služeb a zprostit se odpovědnosti za škody vyplývající z využívání služeb nad rámec těchto omezení. Zákazníci by měli být o těchto omezeních předem řádně informováni. Tato omezení by měla být rozpoznatelná pro třetí osoby, například tím, že informace o těchto omezeních budou zahrnuty v podmínkách poskytované služby, nebo jinými rozpoznatelnými prostředky. Za účelem účinného uplatňování těchto zásad by se toto nařízení mělo použít v souladu s vnitrostátními pravidly odpovědnosti. Tato vnitrostátní pravidla týkající se například vymezení škody, úmyslu nebo nedbalosti nebo související platná procesní pravidla proto tímto nařízením nejsou dotčena.

(38) Oznamování narušení bezpečnosti a posuzování bezpečnostních rizik je nezbytné, aby mohly být dotčeným stranám v případě narušení bezpečnosti nebo ztráty integrity poskytnuty náležité informace.

(39) Aby mohly 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 Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA).

(40) Aby mohly 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 základní požadavky na dohled ve všech členských státech uplatňovány jednotně a účinně.

(41) K zajištění udržitelnosti a stálosti kvalifikovaných služeb vytvářejících důvěru a posílení důvěry uživatelů v kontinuitu kvalifikovaných služeb vytvářejících důvěru by orgány dohledu měly ověřovat existenci a správné uplatňování předpisů o plánech ukončení činnosti v případech, kdy kvalifikovaní poskytovatelé služeb vytvářejících důvěru ukončí svou činnost.

(42) K usnadnění dohledu nad kvalifikovanými poskytovateli služeb vytvářejících důvěru například v případě, že poskytovatel poskytuje své služby na území jiného členského státu a nepodléhá v něm 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.

(43) Aby bylo zajištěno, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované služby splňují požadavky stanovené v tomto nařízení, měl by subjekt posuzování shody provádět posuzování shody a kvalifikovaní poskytovatelé služeb vytvářejících důvěru by měli výsledné zprávy o posouzení shody předkládat orgánu dohledu. Kdykoli orgán dohledu požaduje, aby kvalifikovaný poskytovatel služeb vytvářejících důvěru předložil ad hoc zprávu o posouzení shody, měl by tento orgán dohledu dodržovat zejména zásadu řádné správy věcí veřejných, včetně povinnosti zdůvodnit svá rozhodnutí, a dále zásadu proporcionality. Orgán dohledu by tedy měl svá rozhodnutí požadující ad hoc posouzení shody řádně odůvodnit.

(44) Cílem tohoto nařízení je zajistit soudržný rámec, který by v souvislosti se službami vytvářejícími důvěru zabezpečil vysokou úroveň bezpečnosti a právní jistotu. V tomto směru by při úpravě posuzování shody produktů a služeb měla Komise ve vhodných případech usilovat o synergie se stávajícími příslušnými evropskými a mezinárodními režimy, jako je například nařízení Evropského parlamentu a Rady (ES) č. 765/2008 [1], které stanoví požadavky na akreditaci subjektů posuzování shody a dozor nad trhem s výrobky.

[1] Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

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

(46) Nezbytnými prvky při budování důvěry mezi tržními subjekty jsou důvěryhodné seznamy, jelikož udávají stav kvalifikace poskytovatele služeb v době dohledu.

(47) Důvěra v on-line služby a pohodlí, které tyto služby nabízejí, jsou zásadní pro to, aby mohli uživatelé plně využívat elektronických služeb a vědomě se na ně spoléhat. Za tímto účelem by měla být vytvořena značka důvěry EU, jež by označovala kvalifikované služby vytvářející důvěru poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru. Tato značka důvěry EU pro kvalifikované služby vytvářející důvěru by tyto služby jasně odlišila od ostatních služeb vytvářejících důvěru, a tím by přispěla k transparentnosti na trhu. Používání značky důvěry EU kvalifikovanými poskytovateli služeb vytvářejících důvěru by mělo být dobrovolné a nemělo by vést k uložení žádných jiných požadavků kromě těch, které jsou stanoveny v tomto nařízení.

(48) Ačkoliv k zajištění vzájemného uznávání elektronických podpisů je zapotřebí vysoká úroveň bezpečnosti, měly by být ve zvláštních případech, například v kontextu rozhodnutí Komise 2009/767/ES [1], přijímány rovněž elektronické podpisy s nižší zárukou bezpečnosti.

(49) Toto nařízení by mělo zavést zásadu, že elektronickému podpisu by neměly být upírány právní účinky na základě skutečnosti, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Právní účinky elektronických podpisů v členských státech by však měly být vymezeny vnitrostátním právem, s výjimkou požadavků stanovených v tomto nařízení, podle něhož by měl mít kvalifikovaný elektronický podpis rovnocenný právní účinek jako podpis vlastnoruční.

(50) 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 pečetě, bude obdobně nutné zajistit, aby podporovaly přinejmenším určitý počet formátů zaručených elektronických pečetí.

(51) Podepisující osoba by měla mít možnost svěřit kvalifikované prostředky pro vytváření elektronických podpisů 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 elektronických podpisů, a použitím tohoto prostředku jsou splněny požadavky na kvalifikovaný elektronický podpis.

(52) Vytváření elektronického podpisu na dálku, jehož prostředí spravuje poskytovatel služeb vytvářejících důvěru jménem podepisující osoby, přináší mnohé ekonomické výhody, a bude tedy pravděpodobně stále častější. Aby však bylo zajištěno, že tyto elektronické podpisy budou z právního hlediska uznávány stejně jako elektronické podpisy, které jsou vytvářeny v prostředí spravovaném výlučně uživatelem, měli by poskytovatelé nabízející služby elektronického podpisu na dálku uplatňovat zvláštní postupy pro zajištění bezpečnosti v oblasti řízení a správy a používat důvěryhodné systémy a produkty zahrnující zabezpečené kanály pro elektronickou komunikaci, a zajistit tak spolehlivost prostředí, v němž jsou elektronické podpisy vytvářeny, a zaručit, že je toto prostředí používáno pod výlučnou kontrolou podepisující osoby. V případě kvalifikovaného elektronického podpisu vytvořeného pomocí prostředku pro vytváření elektronických podpisů na dálku by se měly použít požadavky stanovené v tomto nařízení, které jsou použitelné na kvalifikované poskytovatele služeb vytvářejících důvěru.

[1] 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 (Úř. věst. L 274, 20.10.2009, s. 36).

(53) Pozastavení platnosti kvalifikovaných certifikátů je jedním ze zavedených operativních postupů poskytovatelů služeb vytvářejících důvěru v řadě členských států, který se liší od zneplatnění a znamená dočasnou ztrátu platnosti certifikátu. V zájmu právní jistoty je nezbytné, aby bylo pozastavení platnosti certifikátu vždy jasně vyznačeno. Za tímto účelem by měli být poskytovatelé služeb vytvářejících důvěru odpovědní za jasné vyznačení statusu certifikátu a – v případě jeho pozastavení jeho platnosti – přesné doby, na kterou byla platnost certifikátu pozastavena. Toto nařízení by nemělo poskytovatelům služeb vytvářejících důvěru ani členským státům ukládat povinnost pozastavení platnosti uplatňovat, ale mělo by stanovit transparentní pravidla ohledně toho, kdy a kde je tento postup k dispozici.

(54) Pro přeshraniční uznávání kvalifikovaných elektronických podpisů jsou předpokladem přeshraniční interoperabilita a uznávání kvalifikovaných certifikátů. Kvalifikované certifikáty by proto neměly podléhat žádným závazným požadavkům, které přesahují požadavky stanovené v tomto nařízení. Na vnitrostátní úrovni by však zahrnutí zvláštních atributů, například jedinečných identifikátorů, do kvalifikovaných certifikátů mělo být povoleno, pokud tyto zvláštní atributy nebrání přeshraniční interoperabilitě a uznávání kvalifikovaných certifikátů a kvalifikovaných elektronických podpisů.

(55) Certifikace bezpečnosti IT systémů založená na mezinárodních normách, jako jsou ISO 15408 a související hodnotící metody a mechanismy vzájemného uznávání, je důležitým nástrojem ověřování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a měla by být podporována. Inovační řešení a služby, jako například podepisování prostřednictvím mobilního telefonu a podepisování v cloudech, se však opírají o technická a organizační řešení pro kvalifikované prostředky pro vytváření elektronických podpisů, pro něž bezpečnostní normy dosud nemusí být k dispozici nebo pro něž první certifikace bezpečnosti IT systémů dosud probíhá. Pouze v případě, že bezpečnostní normy nejsou k dispozici nebo první certifikace bezpečnosti IT systémů probíhá, by mohla být úroveň bezpečnosti těchto kvalifikovaných prostředků pro vytváření elektronických podpisů posouzena alternativními postupy. Tyto postupy by měly být srovnatelné s normami pro certifikaci bezpečnosti IT systémů, pokud jsou jejich úrovně bezpečnosti rovnocenné. Vzájemné hodnocení by mohlo tyto postupy usnadnit.

(56) Toto nařízení by mělo stanovit požadavky na kvalifikované prostředky pro vytváření elektronických podpisů, které mají zajistit funkčnost zaručených elektronických podpisů. Toto nařízení by nemělo zahrnovat celé systémové prostředí, ve kterém se tyto prostředky využívají. Rozsah certifikace kvalifikovaných prostředků pro vytváření podpisů by proto měl být omezen na technické zařízení a systémové programové vybavení používané pro správu a ochranu dat pro vytváření podpisů, která jsou v prostředku pro vytváření podpisů vytvořena, uložena nebo zpracovávána. Jak je podrobně uvedeno v příslušných normách, měly by být z certifikační povinnosti vyloučeny aplikace pro vytváření podpisů.

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

(58) Vyžaduje-li transakce kvalifikovanou elektronickou pečeť právnické osoby, měl by být stejně tak přijatelný kvalifikovaný elektronický podpis oprávněného zástupce této právnické osoby.

(59) Elektronické pečetě by měly sloužit jako důkaz toho, že elektronický dokument vydala určitá právnická osoba, a poskytovat jistotu o původu a integritě dokumentu.

(60) Poskytovatelé služeb vytvářejících důvěru vydávající kvalifikované certifikáty pro elektronické pečetě by měli zavést nezbytná opatření, aby byli schopni určit totožnost fyzické osoby zastupující právnickou osobu, které je kvalifikovaný certifikát pro elektronickou pečeť poskytován, je-li tato identifikace nezbytná na vnitrostátní úrovni v soudním nebo správním řízení.

(61) Toto nařízení by mělo zajistit dlouhodobé uchovávání informací, aby zajistilo dlouhodobou platnost elektronických podpisů a elektronických pečetí a zaručilo, že mohou být ověřeny bez ohledu na budoucí technologické změny.

(62) Aby byla zajištěna bezpečnost kvalifikovaných elektronických časových razítek, mělo by toto nařízení vyžadovat použití zaručené elektronické pečeti nebo zaručeného elektronického podpisu nebo jiných rovnocenných metod. Lze předpokládat, že inovace mohou vést ke vzniku nových technologií, jež mohou zajistit rovnocennou úroveň bezpečnosti pro časová razítka. Kdykoli je použita jiná metoda než zaručená elektronická pečeť nebo zaručený elektronický podpis, mělo by být na kvalifikovaném poskytovateli služeb vytvářejících důvěru, aby ve zprávě o posouzení shody prokázal, že daná metoda zajišťuje rovnocennou úroveň bezpečnosti a splňuje povinnosti stanovené v tomto nařízení.

(63) Elektronické dokumenty jsou důležité pro další rozvoj přeshraničních elektronických transakcí na vnitřním trhu. Toto nařízení by mělo stanovit zásadu, že elektronickému dokumentu nesmějí být upírány právní účinky na základě skutečnosti, že má elektronickou podobu; cílem této zásady je zajistit, aby elektronická transakce nebyla odmítnuta jen z toho důvodu, že dokument má elektronickou podobu.

(64) Při úpravě formátů zaručených elektronických podpisů a pečetí by Komise měla vycházet ze stávajících postupů, norem a právních předpisů, zejména z rozhodnutí Komise 2011/130/EU ([1]).

(65) Vedle ověření pravosti dokumentu vydaného právnickou osobou lze elektronické pečetě použít k autentizaci jakéhokoli digitálního předmětu dotyčné právnické osoby, například softwarového kódu nebo serverů.

(66) Je nezbytné stanovit právní rámec, který usnadní přeshraniční uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy. Tento rámec by mohl rovněž přinést nové tržní příležitosti pro poskytovatele služeb vytvářejících důvěru z Unie, kteří budou moci nabízet nové panevropské služby elektronického doporučeného doručování.

(67) Služby autentizace internetových stránek poskytují prostředek, s jehož pomocí se návštěvník určitých internetových stránek může ujistit, že tyto stránky reprezentují skutečný a legitimní subjekt. Tyto služby přispívají k budování důvěryhodnosti a důvěry v on-line obchodování, neboť uživatelé budou mít důvěru v internetové stránky, které byly autentizovány. Poskytování a využívání služeb autentizace internetových stránek je zcela dobrovolné. Aby se však autentizace internetových stránek stala prostředkem pro posílení důvěryhodnosti, zlepšení zkušeností uživatelů a podporu růstu na vnitřním trhu, mělo by toto nařízení stanovit pro poskytovatele a jejich služby minimální povinnosti v oblasti bezpečnosti a odpovědnosti. Za tímto účelem byly zohledněny výsledky dosavadních iniciativ vedených odvětvím, jako například fóra pro certifikační orgány a vyhledávače – fórum CA/B. Kromě toho by toto nařízení nemělo bránit používání jiných prostředků nebo metod pro autentizaci internetových stránek, na které se toto nařízení nevztahuje, ani by nemělo poskytovatelům služeb autentizace internetových stránek pocházejícím ze třetích zemí bránit v tom, aby své služby poskytovali zákazníkům v Unii. Služby autentizace internetových stránek nabízené poskytovatelem ze třetí země by však měly být uznány jako kvalifikované služby podle tohoto nařízení pouze v případě, že byla uzavřena mezinárodní dohoda mezi Unií a zemí, v níž je poskytovatel usazen.

(68) Pojetí „právnických osob“ podle ustanovení Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“) týkajících se usazování ponechává hospodářským subjektům možnost volby právní formy, kterou považují za vhodnou pro výkon své činnosti. „Právnickými osobami“ ve smyslu Smlouvy o fungování EU se tedy rozumějí všechny subjekty, které byly založeny podle práva některého členského státu nebo se tímto právem řídí, bez ohledu na jejich právní formu.

(69) Orgány, instituce a jiné subjekty Unie se vybízejí, aby pro účely správní spolupráce uznávaly elektronickou identifikaci a služby vytvářející důvěru upravené tímto nařízením a využívaly přitom zejména stávajících osvědčených postupů a výsledků probíhajících projektů v oblastech, jichž se toto nařízení týká.

([1]) Rozhodnutí Komise 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu (Úř. věst. L 53, 26.2.2011, s. 66).

(70) 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 EU, pokud jde o kritéria, která musí splňovat subjekty odpovědné za certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni. 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.

(71) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, zejména k určení referenčních čísel norem, jejichž použití zakládá předpoklad shody s určitými požadavky stanovenými v tomto nařízení. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ([1]).

(72) Při přijímání aktů v přenesené pravomoci nebo prováděcích aktů by Komise měla řádně zohlednit normy a technické specifikace vypracované evropskými a mezinárodními normalizačními organizacemi a subjekty, zejména pak Evropským výborem pro normalizaci (CEN), Evropským ústavem pro telekomunikační normy (ETSI), Mezinárodní organizací pro normalizaci (ISO) a Mezinárodní telekomunikační unií (ITU), s cílem zajistit vysokou úroveň bezpečnosti a interoperability elektronické identifikace a služeb vytvářejících důvěru.

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

(74) V zájmu zajištění právní jistoty pro tržní subjekty, které již používají kvalifikovaná osvědčení vydaná fyzickým osobám podle směrnice 1999/93/ES, je nutné stanovit dostatečně dlouhou lhůtu pro přechod. Obdobně by měla být stanovena přechodná opatření pro bezpečné prostředky pro vytváření podpisů, jejichž shoda byla zjištěna v souladu se směrnicí 1999/93/ES, a pro ověřovatele, kteří vydávají kvalifikované certifikáty před 1. červencem 2016. V neposlední řadě je rovněž nezbytné umožnit Komisi přijímání prováděcích aktů a aktů v přenesené pravomoci před tímto dnem.

(75) Dny použitelnosti stanovenými v tomto nařízení nejsou dotčeny stávající povinnosti, které členské státy již mají podle právních předpisů Unie, zejména pak podle směrnice 2006/123/ES.

(76) Jelikož cílů tohoto nařízení nemůže být dosaženo uspokojivě členskými státy, ale spíše jich, z důvodu rozsahu opatření, může být 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 těchto cílů.

(77) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 28 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ([2]) a vydal stanovisko dne 27. září 2012 ([3]),

([1]) Nařízení 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 (Úř. věst. L 55, 28.2.2011, s. 13).

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

([3]) Úř. věst. C 28, 30.1.2013, s. 6.

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

S cílem zajistit řádné fungování vnitřního trhu a současně usilovat o odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru toto nařízení:

a) stanoví podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu;

b) stanoví pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí; a

c) stanoví právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na systémy elektronické identifikace oznámené členskými státy a na poskytovatele služeb vytvářejících důvěru usazené v Unii.

2. Toto nařízení se nevztahuje na poskytování služeb vytvářejících důvěru, které jsou používány výhradně v rámci uzavřených systémů vyplývajících z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků.

3. Tímto nařízením není dotčeno vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „elektronickou identifikací“ postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu;

2) „prostředkem pro elektronickou identifikaci“ hmotná či nehmotná jednotka obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby;

3) „osobními identifikačními údaji“ soubor údajů umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující právnickou osobu;

4) „systémem elektronické identifikace“ systém pro elektronickou identifikaci, na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci;

5) „autentizací“ elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě;

6) „spoléhající se stranou“ fyzická nebo právnická osoba, která se spoléhá na elektronickou identifikaci nebo službu vytvářející důvěru;

7) „subjektem veřejného sektoru“ státní, regionální nebo místní orgán, veřejnoprávní subjekt, sdružení vytvořené jedním nebo několika takovými orgány nebo jedním nebo několika takovými veřejnoprávními subjekty nebo soukromý subjekt, který byl alespoň jedním z těchto orgánů, subjektů nebo sdružení pověřen poskytovat veřejné služby, jedná-li na základě tohoto pověření;

8) „veřejnoprávním subjektem“ subjekt vymezený v čl. 2 odst. 1 bodě 4 směrnice Evropského parlamentu a Rady 2014/24/EU ([1]);

9) „podepisující osobou“ fyzická osoba, která vytváří elektronický podpis;

10) „elektronickým podpisem“ data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání;

11) „zaručeným elektronickým podpisem“ elektronický podpis, který splňuje požadavky stanovené v článku 26;

12) „kvalifikovaným elektronickým podpisem“ zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy;

13) „daty pro vytváření elektronických podpisů“ jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů;

14) „certifikátem pro elektronický podpis“ elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby;

15) „kvalifikovaným certifikátem pro elektronický podpis“ certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I;

16) „službou vytvářející důvěru“ elektronická služba, která je zpravidla poskytována za úplatu a spočívá:

   a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo

   b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo

   c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami;

17) „kvalifikovanou službou vytvářející důvěru“ služba vytvářející důvěru, která splňuje použitelné požadavky stanovené v tomto nařízení;

([1]) Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES (Úř. věst. L 94, 28.3.2014, s. 65).

18) „subjektem posuzování shody“ subjekt vymezený v čl. 2 bodě 13 nařízení (ES) č. 765/2008, který je v souladu s uvedeným nařízením akreditován jako způsobilý provádět posuzování shody kvalifikovaného poskytovatele služeb vytvářejících důvěru a jím poskytovaných kvalifikovaných služeb vytvářejících důvěru;

19) „poskytovatelem služeb vytvářejících důvěru“ fyzická nebo právnická osoba, která poskytuje jednu či více služeb vytvářejících důvěru buď jako kvalifikovaný, nebo jako nekvalifikovaný poskytovatel služeb vytvářejících důvěru;

20) „kvalifikovaným poskytovatelem služeb vytvářejících důvěru“ poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele;

21) „produktem“ technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru;

22) „prostředkem pro vytváření elektronických podpisů“ konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů;

23) „kvalifikovaným prostředkem pro vytváření elektronických podpisů“ prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II;

24) „pečetící osobou“ právnická osoba, která vytváří elektronickou pečeť;

25) „elektronickou pečetí“ data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu;

26) „zaručenou elektronickou pečetí“ elektronická pečeť, která splňuje požadavky stanovené v článku 36;

27) „kvalifikovanou elektronickou pečetí“ zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť;

28) „daty pro vytváření elektronických pečetí“ jedinečná data, která pečetící osoba používá k vytváření elektronických pečetí;

29) „certifikátem pro elektronickou pečeť“ elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou a potvrzuje název této osoby;

30) „kvalifikovaným certifikátem pro elektronickou pečeť“ certifikát pro elektronickou pečeť, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze III;

31) „prostředkem pro vytváření elektronických pečetí“ konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických pečetí;

32) „kvalifikovaným prostředkem pro vytváření elektronických pečetí“ prostředek pro vytváření elektronických pečetí, který přiměřeně splňuje požadavky stanovené v příloze II;

33) „elektronickým časovým razítkem“ data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku;

34) „kvalifikovaným elektronickým časovým razítkem“ elektronické časové razítko, které splňuje požadavky stanovené v článku 42;

35) „elektronickým dokumentem“ jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka;

36) „službou elektronického doporučeného doručování“ služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn;

37) „kvalifikovanou službou elektronického doporučeného doručování“ služba elektronického doporučeného doručování, která splňuje požadavky stanovené v článku 44;

38) „certifikátem pro autentizaci internetových stránek“ potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán;

39) „kvalifikovaným certifikátem pro autentizaci internetových stránek“ certifikát pro autentizaci internetových stránek, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze IV;

40) „daty pro ověřování platnosti“ data, která se používají k ověření platnosti elektronického podpisu nebo elektronické pečeti;

41) „ověřováním platnosti“ postup ověřující shodu a potvrzující platnost elektronického podpisu nebo elektronické pečeti.

Článek 4

Zásada vnitřního trhu

1. Nesmějí existovat žádná omezení týkající se poskytování služeb vytvářejících důvěru na území určitého členského státu poskytovatelem služeb vytvářejících důvěru, který je usazen v jiném členském státě, z důvodů spadajících do oblastí, na něž se vztahuje toto nařízení.

2. Produkty a služby vytvářející důvěru, které vyhovují tomuto nařízení, se mohou volně pohybovat na vnitřním trhu.

Článek 5

Zpracování a ochrana údajů

1. Zpracování osobních údajů se provádí v souladu se směrnicí 95/46/ES.

2. Aniž jsou dotčeny právní účinky, které vnitrostátní právo přiznává pseudonymům, není používání pseudonymů v elektronických transakcích zakázáno.

KAPITOLA II

ELEKTRONICKÁ IDENTIFIKACE

Článek 6

Vzájemné uznávání

1. Pokud se podle vnitrostátního práva nebo správní praxe pro přístup ke službě poskytované on-line subjektem veřejného sektoru v určitém členském státě vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizace, je pro účely přeshraniční autentizace pro danou on-line službu uznán v tomto členském státě prostředek pro elektronickou identifikaci vydaný v jiném členském státě, pokud jsou splněny tyto podmínky:

a) daný prostředek pro elektronickou identifikaci je vydán v rámci systému elektronické identifikace, který je uveden na seznamu zveřejněném Komisí podle článku 9;

b) úroveň záruky daného prostředku pro elektronickou identifikaci odpovídá stejné úrovni záruky, jako je úroveň záruky požadovaná příslušným subjektem veřejného sektoru v prvním členském státě pro přístup k dané on-line službě, nebo vyšší úrovni, pokud úroveň záruky daného prostředku pro elektronickou identifikaci odpovídá značné nebo vysoké úrovni záruky;

c) příslušný subjekt veřejného sektoru používá v souvislosti s přístupem k dané on-line službě značnou nebo vysokou úroveň záruky.

K tomuto uznání dojde do dvanácti měsíců od zveřejnění seznamu uvedeného v prvním pododstavci písm. a) Komisí.

2. Pro účely přeshraniční autentizace pro on-line službu poskytovanou subjekty veřejného sektoru mohou tyto subjekty uznat prostředek pro elektronickou identifikaci, který byl vydán v rámci systému elektronické identifikace uvedeného na seznamu zveřejněném Komisí podle článku 9 a který odpovídá nízké úrovni záruky.

Článek 7

Způsobilost systémů elektronické identifikace pro oznámení

Systém elektronické identifikace je způsobilý pro oznámení podle čl. 9 odst. 1, jsou-li splněny všechny tyto podmínky:

a) prostředky pro elektronickou identifikaci v rámci daného systému elektronické identifikace:

i) vydává oznamující členský stát;

ii) jsou vydávány z pověření oznamujícího členského státu; nebo

iii) jsou vydávány nezávisle na oznamujícím členském státu a tento členský stát je uznává;

b) prostředky pro elektronickou identifikaci v rámci daného systému elektronické identifikace lze použít pro přístup k alespoň jedné službě poskytované subjektem veřejného sektoru, u níž se v oznamujícím členském státě vyžaduje elektronická identifikace;

c) daný systém elektronické identifikace a prostředky pro elektronickou identifikaci v rámci tohoto systému vydávané splňují požadavky alespoň na jednu z úrovní záruky stanovených v prováděcím aktu uvedeném v čl. 8 odst. 3;

d) oznamující členský stát zajišťuje, aby osobní identifikační údaje jedinečně identifikující danou osobu byly v okamžiku vydání prostředku pro elektronickou identifikaci v rámci daného systému v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými v prováděcím aktu uvedeném v čl. 8 odst. 3 spojeny s fyzickou nebo právnickou osobou uvedenou v čl. 3 bodě 1;

e) strana vydávající prostředky pro elektronickou identifikaci v rámci daného systému zajišťuje, aby byl prostředek pro elektronickou identifikaci spojen s osobou uvedenou v písmeni d) tohoto článku v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými v prováděcím aktu uvedeném v čl. 8 odst. 3;

f) oznamující členský stát zajišťuje dostupnost on-line autentizace tak, aby kterákoli spoléhající se strana usazená na území jiného členského státu byla schopna potvrdit osobní identifikační údaje, které obdržela v elektronické podobě.

V případě jiných spoléhajících se stran než subjektů veřejného sektoru může oznamující členský stát stanovit podmínky přístupu k této autentizaci. Tato přeshraniční autentizace se poskytuje bezplatně, pokud je prováděna v souvislosti s on-line službou poskytovanou subjektem veřejného sektoru.

Členské státy nesmějí spoléhajícím se stranám, které chtějí tuto autentizaci provést, ukládat zvláštní nepřiměřené technické požadavky, které by bránily interoperabilitě oznámených systémů elektronické identifikace nebo by ji významně ztěžovaly;

g) nejméně šest měsíců před oznámením podle čl. 9 odst. 1 poskytne oznamující členský stát ostatním členským státům pro účely povinnosti stanovené v čl. 12 odst. 5 popis daného systému v souladu s procesními opatřeními stanovenými v prováděcích aktech uvedených v čl. 12 odst. 7;

h) daný systém elektronické identifikace splňuje požadavky stanovené v prováděcím aktu uvedeném v čl. 12 odst. 8.

Článek 8

Úrovně záruky systémů elektronické identifikace

1. Systém elektronické identifikace oznámený podle čl. 9 odst. 1 uvádí nízkou, značnou nebo vysokou úroveň záruky pro prostředky pro elektronickou identifikaci vydávané v rámci tohoto systému.

2. Nízká, značná a vysoká úroveň záruky musí splňovat tato příslušná kritéria:

a) nízká úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí omezenou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je snížit riziko zneužití nebo změny totožnosti;

b) značná úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí značnou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je značně snížit riziko zneužití nebo změny totožnosti;

c) vysoká úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí vyšší míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby než prostředek pro elektronickou identifikaci se značnou úrovní záruky a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je předejít zneužití nebo změně totožnosti.

3. Do 18. září 2015 Komise prostřednictvím prováděcích aktů s přihlédnutím k příslušným mezinárodním normám a s výhradou odstavce 2 stanoví minimální technické specifikace, normy a postupy, jejichž pomocí jsou pro účely odstavce 1 vymezeny nízká, značná a vysoká úroveň záruky prostředků pro elektronickou identifikaci.

Tyto minimální technické specifikace, normy a postupy se stanoví na základě spolehlivosti a kvality:

a) postupu prokazování a ověřování totožnosti fyzických nebo právnických osob žádajících o vydání prostředku pro elektronickou identifikaci;

b) postupu vydávání požadovaných prostředků pro elektronickou identifikaci;

c) mechanismu autentizace, při níž fyzická nebo právnická osoba používá prostředek pro elektronickou identifikaci k tomu, aby spoléhající se straně potvrdila svou totožnost;

d) subjektu vydávajícího prostředky pro elektronickou identifikaci;

e) jakéhokoli jiného subjektu zapojeného do žádosti o vydání prostředku pro elektronickou identifikaci a

f) technických a bezpečnostních specifikací vydaného prostředku pro elektronickou identifikaci.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 9

Oznámení

1. Oznamující členský stát oznámí Komisi tyto informace a bez zbytečného odkladu i jejich případné následné změny:

a) popis systému elektronické identifikace, včetně jeho úrovní záruky a vydavatele či vydavatelů prostředků pro elektronickou identifikaci v rámci tohoto systému;

b) použitelný režim dohledu a informace o režimu odpovědnosti, pokud jde o:

i) stranu vydávající prostředky pro elektronickou identifikaci a

ii) stranu provozující postup autentizace;

c) orgán nebo orgány odpovědné za systém elektronické identifikace;

d) informace o subjektu či subjektech, které spravují evidenci jedinečných osobních identifikačních údajů;

e) popis způsobu, jakým jsou plněny požadavky stanovené v prováděcích aktech uvedených v čl. 12 odst. 8;

f) popis autentizace podle čl. 7 písm. f);

g) opatření k pozastavení platnosti nebo zrušení oznámeného systému elektronické identifikace nebo autentizace či dotčených ohrožených součástí.

2. Jeden rok ode dne použitelnosti prováděcích aktů uvedených v čl. 8 odst. 3 a čl. 12 odst. 8 zveřejní Komise v *Úředním věstníku Evropské unie* seznam systémů elektronické identifikace, které byly oznámeny podle odstavce 1 tohoto článku, a základní informace o těchto systémech.

3. Obdrží-li Komise oznámení po uplynutí lhůty uvedené v odstavci 2, zveřejní změny v seznamu podle uvedeného odstavce v *Úředním věstníku Evropské unie* do dvou měsíců od obdržení daného oznámení.

4. Členský stát může Komisi požádat o vyškrtnutí systému elektronické identifikace, který oznámil, ze seznamu uvedeného v odstavci 2. Do jednoho měsíce od obdržení žádosti členského státu zveřejní Komise odpovídající změny v seznamu v *Úředním věstníku Evropské unie*.

5. Komise může prostřednictvím prováděcích aktů stanovit okolnosti, formáty a postupy pro oznamování podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 10

Narušení bezpečnosti

1. Je-li bezpečnost systému elektronické identifikace oznámeného v souladu s čl. 9 odst. 1 či autentizace uvedené v čl. 7 písm. f) narušena nebo částečně ohrožena způsobem, který ovlivňuje spolehlivost přeshraniční autentizace tohoto systému, oznamující členský stát bezodkladně pozastaví nebo zruší tuto přeshraniční autentizaci nebo dotčené ohrožené součásti a uvědomí o tom ostatní členské státy a Komisi.

2. Pokud bylo narušení nebo ohrožení bezpečnosti uvedené v odstavci 1 napraveno, oznamující členský stát přeshraniční autentizaci obnoví a bez zbytečného odkladu o tom uvědomí ostatní členské státy a Komisi.

3. Pokud k nápravě narušení nebo ohrožení bezpečnosti uvedeného v odstavci 1 nedojde do tří měsíců od pozastavení či zrušení, oznámí oznamující stát ostatním členským státům a Komisi stažení systému elektronické identifikace.

Komise bez zbytečného odkladu zveřejní v *Úředním věstníku Evropské unie* odpovídající změny v seznamu uvedeném v čl. 9 odst. 2.

Článek 11

Odpovědnost za škodu

1. Oznamující členský stát odpovídá za škodu, kterou úmyslně nebo z nedbalosti způsobí kterékoli fyzické nebo právnické osobě nesplněním svých povinností uvedených v čl. 7 písm. d) a f) v přeshraniční transakci.

2. Strana vydávající prostředky pro elektronickou identifikaci odpovídá za škodu, kterou úmyslně nebo z nedbalosti způsobí kterékoli fyzické nebo právnické osobě nesplněním povinnosti uvedené v čl. 7 písm. e) v přeshraniční transakci.

3. Strana provozující postup autentizace odpovídá za škodu, kterou úmyslně nebo z nedbalosti způsobí kterékoli fyzické nebo právnické osobě nezajištěním správného fungování autentizace podle čl. 7 písm. f) v přeshraniční transakci.

4. Odstavce 1, 2 a 3 se použijí v souladu s vnitrostátními pravidly upravujícími odpovědnost za škodu.

5. Odstavci 1, 2 a 3 není dotčena odpovědnost za škodu, kterou podle vnitrostátního práva nesou účastníci transakce, při níž jsou použity prostředky pro elektronickou identifikaci spadající do systému elektronické identifikace oznámeného podle čl. 9 odst. 1.

Článek 12

Spolupráce a interoperabilita

1. Vnitrostátní systémy elektronické identifikace oznámené podle čl. 9 odst. 1 musí být interoperabilní.

2. Pro účely odstavce 1 se zavede rámec interoperability.

3. Rámec interoperability musí splňovat tato kritéria:

a) usiluje o to, aby byl z technologického hlediska neutrální, a v rámci členského státu nerozlišuje mezi žádnými zvláštními vnitrostátními technickými řešeními elektronické identifikace;

b) je-li to možné, řídí se evropskými a mezinárodními normami;

c) usnadňuje uplatňování zásady ochrany soukromí již od návrhu; a

d) zajišťuje, aby osobní údaje byly zpracovávány v souladu se směrnicí 95/46/ES.

4. Rámec interoperability sestává z:

a) odkazu na minimální technické požadavky týkající se úrovní záruky stanovených v článku 8;

b) mapování vnitrostátních úrovní záruky oznámených systémů elektronické identifikace podle úrovní záruky stanovených v článku 8;

c) odkazu na minimální technické požadavky pro interoperabilitu;

d) odkazu na minimální soubor osobních identifikačních údajů jedinečně identifikujících fyzickou nebo právnickou osobu, který je v systémech elektronické identifikace k dispozici;

e) procesních pravidel;

f) opatření pro řešení sporů; a

g) společných norem provozní bezpečnosti.

5. Členské státy spolupracují ohledně:

a) interoperability systémů elektronické identifikace oznámených podle čl. 9 odst. 1 a systémů elektronické identifikace, jež členské státy hodlají oznámit; a

b) bezpečnosti systémů elektronické identifikace.

6. Spolupráce mezi členskými státy zahrnuje:

a) výměnu informací, zkušeností a osvědčených postupů v oblasti systémů elektronické identifikace, a zejména v oblasti technických požadavků týkajících se interoperability a úrovní záruky;

b) výměnu informací, zkušeností a osvědčených postupů v oblasti práce s úrovněmi záruky systémů elektronické identifikace podle článku 8;

c) vzájemné hodnocení systémů elektronické identifikace, které spadají do oblasti působnosti tohoto nařízení; a

d) posouzení relevantního vývoje v odvětví elektronické identifikace.

7. Komise do 18. března 2015 prostřednictvím prováděcích aktů stanoví nezbytná procesní opatření pro usnadnění spolupráce mezi členskými státy podle odstavců 5 a 6 v zájmu podpory vysoké úrovně důvěryhodnosti a bezpečnosti odpovídající míře rizika.

8. Do 18. března 2015 Komise pro účely stanovení jednotných podmínek pro provádění požadavku podle odstavce 1, s výhradou kritérií stanovených v odstavci 3 a s přihlédnutím k výsledkům spolupráce mezi členskými státy, přijme prováděcí akty týkající se rámce interoperability stanoveného v odstavci 4.

9. Prováděcí akty uvedené v odstavcích 7 a 8 tohoto článku se přijímají přezkumným postupem podle čl. 48 odst. 2.

KAPITOLA III

SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU

ODDÍL 1

Obecná ustanovení

Článek 13

Odpovědnost za škodu a důkazní břemeno

1. Aniž je dotčen odstavec 2, poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení.

Důkazní břemeno, pokud jde o úmysl nebo nedbalost nekvalifikovaného poskytovatele služeb vytvářejících důvěru, nese fyzická nebo právnická osoba uplatňující nárok na náhradu škody podle prvního pododstavce.

V případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že škoda podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.

2. Pokud poskytovatelé služeb vytvářejících důvěru své zákazníky předem řádně informují o omezeních týkajících se využívání jimi poskytovaných služeb a tato omezení jsou rozpoznatelná pro třetí osoby, neodpovídají poskytovatelé služeb vytvářejících důvěru za škody způsobené využíváním služeb nad rámec uvedených omezení.

3. Odstavce 1 a 2 se použijí v souladu s vnitrostátními pravidly upravujícími odpovědnost za škodu.

Článek 14

Mezinárodní aspekty

1. Služby vytvářející důvěru poskytované poskytovateli služeb vytvářejících důvěru usazenými ve třetí zemi se uznávají jako právně rovnocenné kvalifikovaným službám vytvářejícím důvěru poskytovaným kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v Unii, pokud jsou služby vytvářející důvěru pocházející ze třetí země uznány na základě dohody uzavřené mezi Unií a dotyčnou třetí zemí nebo mezinárodní organizací v souladu s článkem 218 Smlouvy o fungování EU.

2. Dohody uvedené v odstavci 1 zejména zajistí, aby:

a) poskytovatelé služeb vytvářejících důvěru v třetí zemi nebo mezinárodní organizaci, s níž je dohoda uzavřena, a jimi poskytované služby vytvářející důvěru splňovali požadavky vztahující se na kvalifikované poskytovatele služeb vytvářejících důvěru usazené v Unii a jimi poskytované kvalifikované služby vytvářející důvěru;

b) kvalifikované služby vytvářející důvěru poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v Unii byly uznány jako právně rovnocenné službám vytvářejícím důvěru poskytovaným poskytovateli služeb vytvářejících důvěru v třetí zemi nebo mezinárodní organizaci, s níž je dohoda uzavřena.

Článek 15

Přístupnost pro osoby se zdravotním postižením

Je-li to proveditelné, měly by být poskytované služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb dostupné osobám se zdravotním postižením.

Článek 16

Sankce

Členské státy stanoví pravidla pro ukládání sankcí za porušení tohoto nařízení. Stanovené sankce musí být účinné, přiměřené a odrazující.

ODDÍL 2

Dohled

Článek 17

Orgán dohledu

1. Členské státy určí orgán dohledu usazený na jejich území nebo po vzájemné dohodě s jiným členským státem orgán dohledu usazený v tomto jiném členském státě. Tento orgán odpovídá za plnění úkolů v oblasti dohledu v členském státě, který provedl určení.

Orgánům dohledu musí být uděleny nezbytné pravomoci a odpovídající zdroje pro plnění jejich úkolů.

2. Členské státy sdělí Komisi názvy a adresy jimi určených orgánů dohledu.

3. Orgán dohledu má tyto úlohy:

a) vykonávat dohled nad kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými na území členského státu, který provedl určení, s cílem zajistit prostřednictvím činností předběžného a následného dohledu, aby tito kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru splňovali požadavky stanovené v tomto nařízení;

b) v případě potřeby přijmout prostřednictvím činností následného dohledu opatření ve vztahu k nekvalifikovaným poskytovatelům služeb vytvářejících důvěru usazeným na území členského státu, který provedl určení, pokud je informován, že tito nekvalifikovaní poskytovatelé služeb vytvářejících důvěru nebo jimi poskytované služby vytvářející důvěru údajně nesplňují požadavky stanovené v tomto nařízení.

4. Pro účely odstavce 3 a s výhradou omezení stanovených v uvedeném odstavci patří mezi úkoly orgánu dohledu zejména tyto činnosti:

a) spolupracovat s ostatními orgány dohledu a poskytovat jim pomoc v souladu s článkem 18;

b) provádět analýzu zpráv o posouzení shody uvedených v čl. 20 odst. 1 a čl. 21 odst. 1;

c) informovat ostatní orgány dohledu a veřejnost o případech narušení bezpečnosti nebo ztráty integrity v souladu s čl. 19 odst. 2;

d) podávat Komisi zprávy o svých hlavních činnostech v souladu s odstavcem 6 tohoto článku;

e) provádět audity kvalifikovaných poskytovatelů služeb vytvářejících důvěru nebo požadovat, aby subjekt posuzování shody provedl posouzení shody těchto poskytovatelů v souladu s čl. 20 odst. 2;

f) spolupracovat s orgány pro ochranu údajů, zejména je bez zbytečného odkladu informovat o výsledcích auditů kvalifikovaných poskytovatelů služeb vytvářejících důvěru, jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů;

g) udělovat poskytovatelům služeb vytvářejících důvěru a jimi poskytovaným službám status kvalifikovaného poskytovatele nebo kvalifikované služby a odnímat tento status v souladu s články 20 a 21;

h) informovat subjekt odpovědný za vnitrostátní důvěryhodný seznam podle čl. 22 odst. 3 o svých rozhodnutích udělit nebo odejmout status kvalifikovaného poskytovatele nebo kvalifikované služby, pokud tento subjekt není rovněž orgánem dohledu;

i) ověřovat existenci a správné uplatňování předpisů o plánech ukončení činnosti v případech, kdy kvalifikovaný poskytovatel služeb vytvářejících důvěru ukončí svou činnost, včetně způsobu zpřístupňování informací v souladu s čl. 24 odst. 2 písm. h);

j) požadovat, aby poskytovatelé služeb vytvářejících důvěru napravili případné neplnění požadavků stanovených v tomto nařízení.

5. Členské státy mohou vyžadovat, aby orgán dohledu zavedl, udržoval a aktualizoval důvěryhodnou infrastrukturu v souladu s podmínkami stanovenými vnitrostátním právem.

6. Do 31. března každého roku předloží každý orgán dohledu Komisi zprávu o svých hlavních činnostech v předchozím kalendářním roce, spolu se shrnutím oznámení o narušení bezpečnosti, která obdržel od poskytovatelů služeb vytvářejících důvěru v souladu s čl. 19 odst. 2.

7. Výroční zprávu uvedenou v odstavci 6 Komise zpřístupní členským státům.

8. Komise může prostřednictvím prováděcích aktů stanovit formáty a postupy pro podávání zpráv podle odstavce 6. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 18

Vzájemná pomoc

1. Orgány dohledu vzájemně spolupracují za účelem výměny osvědčených postupů.

Po obdržení odůvodněné žádosti jiného orgánu dohledu poskytne orgán dohledu danému orgánu pomoc, aby bylo možné zajistit jednotný výkon činností orgánů dohledu. Vzájemná pomoc může zahrnovat zejména žádosti o informace a opatření v oblasti dohledu, například žádosti o provedení prověrek v souvislosti se zprávami o posouzení shody podle článků 20 a 21.

2. Orgán dohledu, jemuž byla podána žádost o pomoc, může tuto žádost zamítnout z kteréhokoliv z těchto důvodů:

a) orgán dohledu není k poskytnutí požadované pomoci příslušný;

b) požadovaná pomoc je nepřiměřená činnostem v oblasti dohledu, které daný orgán dohledu vykonává v souladu s článkem 17;

c) poskytnutí požadované pomoci by nebylo slučitelné s tímto nařízením.

3. Členské státy mohou svým příslušným orgánům dohledu případně povolit provádět společná šetření, na nichž se podílejí pracovníci orgánů dohledu z ostatních členských států. Ujednání a postupy pro tyto společné akce dohodnou a zavedou dotčené členské státy v souladu se svými vnitrostátními právními předpisy.

Článek 19

Bezpečnostní požadavky vztahující se na poskytovatele služeb vytvářejících důvěru

1. Kvalifikovaní a nekvalifikovaní poskytovatelé služeb vytvářejících důvěru přijmou vhodná technická a organizační opatření k řízení rizik ohrožujících bezpečnost jimi poskytovaných služeb vytvářejících důvěru. S ohledem na nejnovější technologický vývoj musí tato opatření zajišťovat úroveň bezpečnosti, která je přiměřená míře rizika. Zejména musí být přijata opatření k zabránění bezpečnostním incidentům, k minimalizaci jejich dopadů a k informování zúčastněných stran o nepříznivých dopadech těchto incidentů.

2. Kvalifikovaní a nekvalifikovaní poskytovatelé služeb vytvářejících důvěru vyrozumí orgán dohledu a případné další příslušné subjekty, jako jsou příslušný vnitrostátní orgán pro bezpečnost informací nebo orgán pro ochranu údajů, o každém narušení bezpečnosti nebo ztrátě integrity, jež mají významný dopad na poskytovanou službu vytvářející důvěru nebo na uchovávané osobní údaje, a to bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy toto narušení zjistili.

Může-li mít narušení bezpečnosti nebo ztráta integrity nepříznivý dopad na fyzickou nebo právnickou osobu, jíž byla služba vytvářející důvěru poskytnuta, vyrozumí poskytovatel služeb vytvářejících důvěru o daném narušení bezpečnosti nebo dané ztrátě integrity bez zbytečného odkladu také tuto fyzickou nebo právnickou osobu.

Je-li to vhodné, zejména týká-li se narušení bezpečnosti nebo ztráta integrity dvou nebo více členských států, uvědomí vyrozuměný orgán dohledu orgány dohledu v ostatních dotčených členských státech a ENISA.

Vyrozuměný orgán dohledu informuje veřejnost nebo požádá, aby tak učinil poskytovatel služeb vytvářejících důvěru, pokud rozhodne, že zveřejnění informací o narušení bezpečnosti nebo ztrátě integrity je ve veřejném zájmu.

3. Orgán dohledu poskytne ENISA jednou ročně shrnutí oznámení o narušení bezpečnosti a ztrátě integrity, která od poskytovatelů služeb vytvářejících důvěru obdržel.

4. Komise může prostřednictvím prováděcích aktů:

a) dále upřesnit opatření uvedená v odstavci 1 a

b) stanovit formáty a postupy, včetně lhůt, použitelné pro účely odstavce 2.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

ODDÍL 3

Kvalifikované služby vytvářející důvěru

Článek 20

Dohled nad kvalifikovanými poskytovateli služeb vytvářejících důvěru

1. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru se na vlastní náklady alespoň jednou za 24 měsíců podrobí auditu ze strany subjektu posuzování shody. Účelem auditu je potvrzení toho, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru předloží výslednou zprávu o posouzení shody do tří pracovních dnů od jejího obdržení orgánu dohledu.

2. Aniž je dotčen odstavec 1, může orgán dohledu u kvalifikovaných poskytovatelů služeb vytvářejících důvěru na jejich náklady kdykoli provést audit nebo požádat subjekt posuzování shody o provedení posouzení shody za účelem potvrzení, že oni sami i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení. Jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů, sdělí orgán dohledu výsledky svých auditů orgánům pro ochranu údajů.

3. Pokud orgán dohledu požaduje, aby kvalifikovaný poskytovatel služeb vytvářejících důvěru napravil neplnění požadavků podle tohoto nařízení, a tento poskytovatel ve lhůtě případně stanovené orgánem dohledu neučiní příslušné kroky, může orgán dohledu zejména s přihlédnutím k rozsahu, délce trvání a důsledkům daného neplnění odejmout danému poskytovateli a jím poskytované dotčené službě status kvalifikovaného poskytovatele nebo kvalifikované služby a informovat o této skutečnosti subjekt uvedený v čl. 22 odst. 3 za účelem aktualizace důvěryhodných seznamů podle čl. 22 odst. 1. Orgán dohledu vyrozumí daného kvalifikovaného poskytovatele služeb vytvářejících důvěru o odnětí statusu kvalifikovaného poskytovatele nebo kvalifikované služby.

4. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro:

a) akreditaci subjektů posuzování shody a pro zprávy o posouzení shody podle odstavce 1;

b) pravidla auditu, podle nichž budou subjekty posuzování shody provádět posuzování shody kvalifikovaných poskytovatelů služeb vytvářejících důvěru podle odstavce 1.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 21

Zahájení poskytování kvalifikované služby vytvářející důvěru

1. Pokud mají poskytovatelé služeb vytvářejících důvěru bez statusu kvalifikovaného poskytovatele v úmyslu začít poskytovat kvalifikované služby vytvářející důvěru, předloží orgánu dohledu oznámení o svém úmyslu společně se zprávou o posouzení shody vydanou subjektem posuzování shody.

2. Orgán dohledu ověří, zda poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení, zejména požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a na jimi poskytované kvalifikované služby vytvářející důvěru.

Dojde-li orgán dohledu k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky uvedené v prvním pododstavci, udělí orgán dohledu tomuto poskytovateli služeb vytvářejících důvěru a jím poskytovaným službám vytvářejícím důvěru status kvalifikovaného poskytovatele nebo kvalifikované služby a uvědomí o tom subjekt uvedený v čl. 22 odst. 3 za účelem aktualizace důvěryhodných seznamů podle čl. 22 odst. 1, a to do tří měsíců od obdržení oznámení podle odstavce 1 tohoto článku.

Není-li ověření dokončeno do tří měsíců od oznámení, vyrozumí orgán dohledu poskytovatele služeb vytvářejících důvěru a uvede důvody prodlení a dobu, v níž bude ověřování dokončeno.

3. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru mohou začít danou kvalifikovanou službu vytvářející důvěru poskytovat poté, co byl status kvalifikovaného poskytovatele nebo kvalifikované služby vyznačen v důvěryhodných seznamech uvedených v čl. 22 odst. 1.

4. Komise může prostřednictvím prováděcích aktů stanovit formáty a postupy pro účely odstavců 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 22

Důvěryhodné seznamy

1. Každý členský stát zřizuje, udržuje a zveřejňuje důvěryhodné seznamy obsahující informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru v jeho působnosti spolu s informacemi o jimi poskytovaných kvalifikovaných službách vytvářejících důvěru.

2. Členské státy zřizují ve formě vhodné pro automatické zpracování, udržují a zabezpečeným způsobem zveřejňují důvěryhodné seznamy uvedené v odstavci 1, které jsou opatřeny elektronickým podpisem nebo elektronickou pečetí.

3. Členské státy bez zbytečného odkladu sdělí Komisi informace o subjektu odpovědném za zřízení, udržování a zveřejnění vnitrostátních důvěryhodných seznamů a poskytnou informace o místě zveřejnění těchto seznamů, o certifikátech použitých k opatření důvěryhodných seznamů elektronickým podpisem nebo pečetí a o jejich případných změnách.

4. Informace uvedené v odstavci 3 Komise bezpečnou cestou zpřístupní veřejnosti ve formě opatřené elektronickým podpisem nebo pečetí a vhodné pro automatické zpracování.

5. Do 18. září 2015 Komise prostřednictvím prováděcích aktů upřesní informace uvedené v odstavci 1 a stanoví technické specifikace a formáty pro důvěryhodné seznamy, které se použijí pro účely odstavců 1 až 4. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 23

Značka důvěry EU pro kvalifikované služby vytvářející důvěru

1. Po vyznačení statusu kvalifikovaného poskytovatele nebo kvalifikované služby podle čl. 21 odst. 2 druhého pododstavce v důvěryhodném seznamu uvedeném v čl. 22 odst. 1 mohou kvalifikovaní poskytovatelé služeb vytvářejících důvěru pomocí značky důvěry EU jednoduchým, rozpoznatelným a jasným způsobem označovat jimi poskytované kvalifikované služby vytvářející důvěru.

2. Pokud kvalifikovaní poskytovatelé služeb vytvářejících důvěru používají pro kvalifikované služby vytvářející důvěru uvedené v odstavci 1 značku důvěry EU, zajistí, aby byl na jejich internetových stránkách k dispozici odkaz na příslušný důvěryhodný seznam.

3. Do 1. července 2015 Komise prostřednictvím prováděcích aktů stanoví specifikace týkající se podoby, a zejména formátu, uspořádání, velikosti a vzhledu značky důvěry EU pro kvalifikované služby vytvářející důvěru. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 24

Požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru

1. Při vydávání kvalifikovaného certifikátu pro službu vytvářející důvěru ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru pomocí vhodných prostředků a v souladu s vnitrostátním právem totožnost a případně zvláštní znaky fyzické nebo právnické osoby, jíž je kvalifikovaný certifikát vydáván.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru ověří informace uvedené v prvním pododstavci přímo nebo tím, že se v souladu s vnitrostátním právem spolehne na třetí osobu:

a) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby; nebo

b) na dálku s využitím prostředku pro elektronickou identifikaci, u něhož byla před vydáním kvalifikovaného certifikátu zajištěna fyzická přítomnost fyzické osoby nebo oprávněného zástupce právnické osoby a jenž splňuje požadavky stanovené v článku 8, pokud jde o značnou nebo vysokou úroveň záruky; nebo

c) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaného v souladu s písmenem a) nebo b); nebo

d) pomocí jiných identifikačních metod uznávaných na vnitrostátní úrovni, které poskytují záruku spolehlivosti rovnocennou fyzické přítomnosti. Tuto rovnocennou záruku musí potvrdit subjekt posuzování shody.

2. Kvalifikovaný poskytovatel služeb vytvářejících důvěru poskytující kvalifikované služby vytvářející důvěru:

a) oznámí orgánu dohledu případné změny v poskytování svých kvalifikovaných služeb vytvářejících důvěru a záměr ukončit své činnosti;

b) zaměstnává pracovníky a případně subdodavatele, kteří mají potřebné odborné znalosti, zkušenosti a kvalifikace, jsou spolehliví a absolvovali odpovídající odbornou přípravu týkající se bezpečnosti a pravidel ochrany osobních údajů, a používá správní a řídicí postupy, které odpovídají evropským nebo mezinárodním normám;

c) vzhledem k riziku odpovědnosti za škody v souladu s článkem 13 udržuje dostatečné finanční prostředky nebo uzavřel vhodné pojištění odpovědnosti v souladu s vnitrostátním právem;

d) před uzavřením smluvního vztahu informuje jasným a srozumitelným způsobem osobu, která chce využít kvalifikovanou službu vytvářející důvěru, o přesných podmínkách používání této služby, včetně případných omezení jejího využívání;

e) používá důvěryhodné systémy a produkty, které jsou chráněny proti pozměnění, a zajišťuje technickou bezpečnost a spolehlivost procesů, které podporují;

f) používá důvěryhodné systémy k uchovávání dat, která jsou mu poskytnuta, v ověřitelné podobě, aby:

i) byla veřejně přístupná pro účely vyhledávání pouze se souhlasem osoby, jíž se data týkají,

ii) záznamy a změny v uložených datech mohly provádět pouze oprávněné osoby,

iii) bylo možno ověřit pravost dat;

g) přijímá vhodná opatření proti padělání a odcizení dat;

h) po přiměřenou dobu, i poté, co ukončil svou činnost kvalifikovaného poskytovatele služeb vytvářejících důvěru, eviduje a zpřístupňuje veškeré příslušné informace týkající se dat, která vydal a obdržel, zejména pro účely poskytnutí důkazů v soudním a správním řízení a pro účely zajištění kontinuity služby. Tato evidence může mít elektronickou podobu;

i) má k dispozici aktualizovaný plán ukončení činnosti k zajištění kontinuity služby v souladu s předpisy ověřenými orgánem dohledu podle čl. 17 odst. 4 písm. i);

j) zajišťuje zákonné zpracovávání osobních údajů v souladu se směrnicí 95/46/ES;

k) pokud se jedná o kvalifikovaného poskytovatele služeb vytvářejících důvěru vydávajícího kvalifikované certifikáty, vede a aktualizuje databázi certifikátů.

3. Jestliže se kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty rozhodne určitý certifikát zneplatnit, zaeviduje toto zneplatnění ve své databázi certifikátů a zneplatnění certifikátu včas a v každém případě do 24 hodin od obdržení žádosti zveřejní. Zneplatnění nabývá účinku okamžitě po zveřejnění.

4. Pokud jde o odstavec 3, kvalifikovaní poskytovatelé služeb vytvářejících důvěru vydávající kvalifikované certifikáty poskytnou kterékoli spoléhající se straně informace o platnosti nebo o zneplatnění kvalifikovaných certifikátů, které vydali. Tyto informace se poskytnou alespoň na základě certifikátu, a to kdykoli i po skončení doby platnosti certifikátu, automatizovaným způsobem, který je spolehlivý, bezplatný a účinný.

5. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro důvěryhodné systémy a produkty, které splňují požadavky podle odst. 2 písm. e) a f) tohoto článku. Pokud důvěryhodné systémy a produkty vyhovují těmto normám, předpokládá se shoda s požadavky stanovenými v tomto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

ODDÍL 4

Elektronický podpis

Článek 25

Právní účinky elektronických podpisů

1. Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.

2. Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.

3. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

Článek 26

Požadavky na zaručené elektronické podpisy

Zaručený elektronický podpis musí splňovat tyto požadavky:

a) je jednoznačně spojen s podepisující osobou;

b) umožňuje identifikaci podepisující osoby;

c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a

d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Článek 27

Elektronické podpisy ve veřejných službách

1. Pokud členský stát pro využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem, požaduje zaručený elektronický podpis, uznává zaručené elektronické podpisy, zaručené elektronické podpisy založené na kvalifikovaném certifikátu pro elektronické podpisy a kvalifikované elektronické podpisy alespoň ve formátech nebo s použitím metod stanovených v prováděcích aktech uvedených v odstavci 5.

2. Pokud členský stát pro využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem, požaduje zaručený elektronický podpis založený na kvalifikovaném certifikátu, uznává zaručené elektronické podpisy založené na kvalifikovaném certifikátu a kvalifikované elektronické podpisy alespoň ve formátech nebo s použitím metod stanovených v prováděcích aktech uvedených v odstavci 5.

3. Členské státy nesmějí v případě přeshraničního využívání on-line služby poskytované subjektem veřejného sektoru vyžadovat elektronický podpis s vyšší zárukou bezpečnosti než kvalifikovaný elektronický podpis.

4. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro zaručené elektronické podpisy. Pokud zaručený elektronický podpis vyhovuje těmto normám, předpokládá se shoda s požadavky na zaručené elektronické podpisy uvedenými v odstavcích 1 a 2 tohoto článku a v článku 26. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

5. Do 18. září 2015 Komise s přihlédnutím ke stávajícím postupům, normám a právním aktům Unie stanoví prostřednictvím prováděcích aktů referenční formáty zaručených elektronických podpisů nebo referenční metody, jsou-li používány alternativní formáty. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 28

Kvalifikované certifikáty pro elektronické podpisy

1. Kvalifikované certifikáty pro elektronické podpisy musí splňovat požadavky stanovené v příloze I.

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

3. Kvalifikované certifikáty pro elektronické podpisy mohou obsahovat další zvláštní atributy, které nejsou povinné. Těmito atributy nesmějí být dotčeny interoperabilita a uznávání kvalifikovaných elektronických podpisů.

4. Pokud byl kvalifikovaný certifikát pro elektronické podpisy po počáteční aktivaci zneplatněn, ztrácí okamžikem zneplatnění platnost a jeho status se nemůže v žádném případě změnit zpět.

5. Členské státy mohou stanovit vnitrostátní pravidla dočasného pozastavení platnosti kvalifikovaných certifikátů pro elektronický podpis s výhradou těchto podmínek:

a) je-li platnost kvalifikovaného certifikátu pro elektronický podpis dočasně pozastavena, pozbývá tento certifikát na dobu pozastavení platnosti;

b) doba pozastavení platnosti je jasně vyznačena v databázi certifikátů a pozastavení platnosti je po svou dobu viditelné ve službě poskytující informace o statusu certifikátu.

6. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikované certifikáty pro elektronický podpis. 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. 48 odst. 2.

Článek 29

Požadavky na kvalifikované prostředky pro vytváření elektronických podpisů

1. Kvalifikované prostředky pro vytváření elektronických podpisů musí splňovat požadavky stanovené v příloze II.

2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikované prostředky pro vytváření elektronických podpisů. Pokud kvalifikovaný prostředek pro vytváření elektronických podpisů vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze II. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 30

Certifikace kvalifikovaných prostředků pro vytváření elektronických podpisů

1. Shodu kvalifikovaných prostředků pro vytváření elektronických podpisů s požadavky stanovenými v příloze II certifikují příslušné veřejné nebo soukromé subjekty, které určily členské státy.

2. Členské státy sdělí Komisi názvy a adresy veřejných nebo soukromých subjektů uvedených v odstavci 1. Komise tyto informace zpřístupní členským státům.

3. Certifikace podle odstavce 1 je založena na jednom z těchto postupů:

a) postupu posouzení bezpečnosti, který byl proveden v souladu s některou z norem pro posuzování bezpečnosti produktů informačních technologií uvedených na seznamu sestaveném v souladu s druhým pododstavcem tohoto odstavce; nebo

b) jiném postupu, než je postup uvedený v písmenu a), za podmínky, že používá srovnatelné úrovně bezpečnosti a že veřejný nebo soukromý subjekt uvedený v odstavci 1 daný postup oznámí Komisi. Tento postup může být použit pouze v případě, že normy uvedené v písmenu a) neexistují nebo že postup posouzení bezpečnosti podle písmene a) dosud probíhá.

Komise prostřednictvím prováděcích aktů sestaví seznam norem pro posuzování bezpečnosti produktů informačních technologií uvedený v prvním pododstavci písm. a). Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

4. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 47, pokud jde o stanovení zvláštních kritérií, která mají splňovat určené subjekty uvedené v odstavci 1 tohoto článku.

Článek 31

Zveřejnění seznamu certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů

1. Členské státy bez zbytečného odkladu a nejpozději jeden měsíc po ukončení certifikace oznámí Komisi informace o kvalifikovaných prostředcích pro vytváření elektronických podpisů, které byly certifikovány subjekty uvedenými v čl. 30 odst. 1. Bez zbytečného odkladu a nejpozději jeden měsíc po zrušení certifikace Komisi rovněž oznámí informace o prostředcích pro vytváření elektronických podpisů, které již nebudou certifikovány.

2. Na základě obdržených informací Komise zřizuje, zveřejňuje a udržuje seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů.

3. Komise může prostřednictvím prováděcích aktů stanovit formáty a postupy použitelné pro účely odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 32

Požadavky na ověřování platnosti kvalifikovaných elektronických podpisů

1. Postup ověření platnosti kvalifikovaného elektronického podpisu potvrdí platnost kvalifikovaného elektronického podpisu, pokud:

a) certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis, jenž je v souladu s přílohou I;

b) kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;

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

d) spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;

e) pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;

f) elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů;

g) nebyla ohrožena integrita podepsaných dat;

h) v okamžiku podpisu byly splněny požadavky stanovené v článku 26.

2. Systém použitý k ověření platnosti kvalifikovaného elektronického podpisu musí poskytovat spoléhající se straně řádný výsledek postupu ověření platnosti a umožňovat jí zjistit jakékoli problémy týkající se bezpečnosti.

3. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro ověřování platnosti kvalifikovaných elektronických podpisů. Pokud ověřování platnosti kvalifikovaných elektronických podpisů vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 33

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů

1. Kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který:

a) zajišťuje ověřování platnosti v souladu s čl. 32 odst. 1 a

b) umožňuje, aby spoléhající se strany obdržely výsledek postupu ověření platnosti automatizovaným způsobem, který je spolehlivý, účinný a je opatřen zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí poskytovatele kvalifikované služby ověřování platnosti.

2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikovanou službu ověřování platnosti uvedenou v odstavci 1. Pokud služba ověřování platnosti kvalifikovaných elektronických podpisů vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 34

Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů

1. Kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který používá postupy a technologie, jež jsou s to zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti.

2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů. Pokud postupy pro kvalifikovanou službu 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. 48 odst. 2.

ODDÍL 5

Elektronické pečetě

Článek 35

Právní účinky elektronických pečetí

1. Elektronické pečeti nesmějí být upírány právní účinky a nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečetě.

2. U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena.

3. Kvalifikovaná elektronická pečeť založená na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaná elektronická pečeť ve všech ostatních členských státech.

Článek 36

Požadavky na zaručené elektronické pečetě

Zaručená elektronická pečeť musí splňovat tyto požadavky:

a) je jednoznačně spojena s pečetící osobou;

b) umožňuje identifikaci pečetící osoby;

c) je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou; a

d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Článek 37

Elektronické pečetě ve veřejných službách

1. Pokud členský stát pro využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem, požaduje zaručenou elektronickou pečeť, uznává zaručené elektronické pečetě, zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě a kvalifikované elektronické pečetě alespoň ve formátech nebo s použitím metod stanovených v prováděcích aktech uvedených v odstavci 5.

2. Pokud členský stát pro využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem, požaduje zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu, uznává zaručené elektronické pečetě založené na kvalifikovaném certifikátu a kvalifikované elektronické pečetě alespoň ve formátech nebo s použitím metod stanovených v prováděcích aktech uvedených v odstavci 5.

3. Členské státy nesmějí v případě přeshraničního využívání on-line služby poskytované subjektem veřejného sektoru vyžadovat elektronickou pečeť s vyšší zárukou bezpečnosti než kvalifikovanou elektronickou pečeť.

4. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro zaručené elektronické pečetě. Pokud zaručená elektronická pečeť vyhovuje těmto normám, předpokládá se shoda s požadavky na zaručené elektronické pečetě uvedenými v odstavcích 1 a 2 tohoto článku a v článku 36. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

5. Do 18. září 2015 Komise s přihlédnutím ke stávajícím postupům, normám a právním aktům Unie stanoví prostřednictvím prováděcích aktů referenční formáty zaručených elektronických pečetí nebo referenční metody, jsou-li používány alternativní formáty. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 38

Kvalifikované certifikáty pro elektronické pečetě

1. Kvalifikované certifikáty pro elektronické pečetě musí splňovat požadavky stanovené v příloze III.

2. Kvalifikované certifikáty pro elektronické pečetě nepodléhají žádným závazným požadavkům, které přesahují požadavky stanovené v příloze III.

3. Kvalifikované certifikáty pro elektronické pečetě mohou obsahovat další zvláštní atributy, které nejsou povinné. Těmito atributy nesmějí být dotčeny interoperabilita a uznávání kvalifikovaných elektronických pečetí.

4. Pokud byl kvalifikovaný certifikát pro elektronickou pečeť po počáteční aktivaci zneplatněn, ztrácí okamžikem zneplatnění platnost a jeho status se nemůže v žádném případě změnit zpět.

5. Členské státy mohou stanovit vnitrostátní pravidla dočasného pozastavení platnosti kvalifikovaných certifikátů pro elektronické pečetě s výhradou těchto podmínek:

a) je-li platnost kvalifikovaného certifikátu pro elektronickou pečeť dočasně pozastavena, pozbývá tento certifikát na dobu pozastavení platnosti;

b) doba pozastavení platnosti je jasně vyznačena v databázi certifikátů a pozastavení platnosti je po svou dobu viditelné ve službě poskytující informace o statusu certifikátu.

6. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikované certifikáty pro elektronické pečetě. Pokud kvalifikovaný certifikát pro elektronickou pečeť vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze III. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 39

Kvalifikované prostředky pro vytváření elektronických pečetí

1. Na kvalifikované prostředky pro vytváření elektronických pečetí se použije přiměřeně článek 29.

2. Na certifikaci kvalifikovaných prostředků pro vytváření elektronických pečetí se použije přiměřeně článek 30.

3. Na zveřejnění seznamu certifikovaných kvalifikovaných prostředků pro vytváření elektronických pečetí se použije přiměřeně článek 31.

Článek 40

Ověřování platnosti a uchovávání kvalifikovaných elektronických pečetí

Na ověřování platnosti a uchovávání kvalifikovaných elektronických pečetí se použijí přiměřeně články 32, 33 a 34.

ODDÍL 6

Elektronická časová razítka

Článek 41

Právní účinek elektronických časových razítek

1. Elektronickému časovému razítku nesmějí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko.

2. U kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny.

3. Kvalifikované elektronické časové razítko vydané v jednom členském státě se uznává jako kvalifikované elektronické časové razítko ve všech členských státech.

Článek 42

Požadavky na kvalifikovaná elektronická časová razítka

1. Kvalifikované elektronické časové razítko musí splňovat tyto požadavky:

a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat;

b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem; a

c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.

2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro spojování data a času s daty a pro zdroje přesného času. Pokud spojení data a 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. 48 odst. 2.

ODDÍL 7

Služba elektronického doporučeného doručování

Článek 43

Právní účinek služby elektronického doporučeného doručování

1. Datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování nesmějí být upírány právní účinky a nesmějí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nesplňují požadavky na kvalifikovanou službu elektronického doporučeného doručování.

2. U dat odeslaných a přijatých prostřednictvím kvalifikované služby elektronického doporučeného doručování platí domněnka integrity dat, odeslání těchto dat identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a správnosti data a času odeslání a přijetí, jež jsou u kvalifikované služby elektronického doporučeného doručování uvedeny.

Článek 44

Požadavky na kvalifikované služby elektronického doporučeného doručování

1. Kvalifikované služby elektronického doporučeného doručování musí splňovat tyto požadavky:

a) jsou poskytovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;

b) s vysokou úrovní spolehlivosti zajišťují identifikaci odesílatele;

c) zajišťují identifikaci příjemce před doručením dat;

d) odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat;

e) odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat;

f) datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného elektronického časového razítka.

V případě přenosu dat mezi dvěma či více kvalifikovanými poskytovateli služeb vytvářejících důvěru se požadavky uvedené v písm. a) až f) vztahují na všechny tyto kvalifikované poskytovatele služeb vytvářejících důvěru.

2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro postupy odesílání a přijímání dat. 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. 48 odst. 2.

ODDÍL 8

Autentizace internetových stránek

Článek 45

Požadavky na kvalifikované certifikáty pro autentizaci internetových stránek

1. Kvalifikované certifikáty pro autentizaci internetových stránek musí splňovat požadavky stanovené v příloze IV.

2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikované certifikáty pro autentizaci internetových stránek. Pokud kvalifikovaný certifikát pro autentizaci internetových stránek vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze IV. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

KAPITOLA IV

ELEKTRONICKÉ DOKUMENTY

Článek 46

Právní účinky elektronických dokumentů

Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.

KAPITOLA V

PŘENESENÍ PRAVOMOCI A PROVÁDĚCÍ USTANOVENÍ

Článek 47

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 uvedené v čl. 30 odst. 4 je svěřena Komisi na dobu neurčitou ode dne 17. září 2014.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 30 odst. 4 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. 30 odst. 4 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.

Článek 48

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 (EU) č. 182/2011.

KAPITOLA VI

ZÁVĚREČNÁ USTANOVENÍ

Článek 49

Přezkum

Do 1. července 2020 přezkoumá Komise uplatňování tohoto nařízení a podá zprávu Evropskému parlamentu a Radě. Komise zejména vyhodnotí, zda je s přihlédnutím ke zkušenostem s uplatňováním tohoto nařízení a k technologickému, tržnímu a právnímu vývoji vhodné upravit oblast působnosti tohoto nařízení nebo jeho konkrétní ustanovení, včetně článku 6, čl. 7 písm. f) a článků 34, 43, 44 a 45.

Ke zprávě uvedené v prvním pododstavci se případně připojí legislativní návrhy.

Vedle toho Komise každé čtyři roky od předložení zprávy uvedené v prvním pododstavci předloží Evropskému parlamentu a Radě zprávu o pokroku v dosahování cílů tohoto nařízení.

Článek 50

Zrušení

1. Směrnice 1999/93/ES se zrušuje s účinkem ode dne 1. července 2016.

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

Článek 51

Přechodná opatření

1. 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 elektronických podpisů podle tohoto nařízení.

2. Kvalifikovaná osvědčení vydaná fyzickým osobám podle směrnice 1999/93/ES se považují za kvalifikované certifikáty pro elektronické podpisy podle tohoto nařízení až do doby skončení jejich platnosti.

3. Ověřovatel vydávající kvalifikovaná osvědčení podle směrnice 1999/93/ES předloží orgánu dohledu co nejdříve, nejpozději však 1. července 2017, zprávu o posouzení shody. Do předložení této zprávy o posouzení shody a dokončení jejího hodnocení orgánem dohledu se ověřovatel považuje za kvalifikovaného poskytovatele služeb vytvářejících důvěru podle tohoto nařízení.

4. Nepředloží-li ověřovatel vydávající kvalifikovaná osvědčení podle směrnice 1999/93/ES orgánu dohledu zprávu o posouzení shody ve lhůtě uvedené v odstavci 3, nepovažuje se tento ověřovatel od 2. července 2017 za kvalifikovaného poskytovatele služeb vytvářejících důvěru podle tohoto nařízení.

Článek 52

Vstup v platnost

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

2. Toto nařízení se použije ode dne 1. července 2016, s těmito výjimkami:

a) čl. 8 odst. 3, čl. 9 odst. 5, čl. 12 odst. 2 až 9, čl. 17 odst. 8, čl. 19 odst. 4, čl. 20 odst. 4, čl. 21 odst. 4, čl. 22 odst. 5, čl. 23 odst. 3, čl. 24 odst. 5, čl. 27 odst. 4 a 5, čl. 28 odst. 6, čl. 29 odst. 2, čl. 30 odst. 3 a 4, čl. 31 odst. 3, čl. 32 odst. 3, čl. 33 odst. 2, čl. 34 odst. 2, čl. 37 odst. 4 a 5, čl. 38 odst. 6, čl. 42 odst. 2, čl. 44 odst. 2, čl. 45 odst. 2 a články 47 a 48 se použijí ode dne 17. září 2014;

b) článek 7, čl. 8 odst. 1 a 2, články 9, 10 a 11 a čl. 12 odst. 1 se použijí ode dne použitelnosti prováděcích aktů uvedených v čl. 8 odst. 3 a čl. 12 odst. 8;

c) článek 6 se použije od uplynutí tří let ode dne použitelnosti prováděcích aktů uvedených v čl. 8 odst. 3 a čl. 12 odst. 8.

3. Pokud je oznámený systém elektronické identifikace na seznamu, který Komise zveřejní podle článku 9, uveden přede dnem uvedeným v odst. 2 písm. c) tohoto článku, dojde k uznání prostředků pro elektronickou identifikaci v rámci tohoto systému podle článku 6 nejpozději dvanáct měsíců po zveřejnění tohoto systému, avšak nejdříve ke dni uvedenému v odst. 2 písm. c) tohoto článku.

4. Bez ohledu na odst. 2 písm. c) tohoto článku může členský stát rozhodnout, že prostředky pro elektronickou identifikaci v rámci systému elektronické identifikace, který jiný členský stát oznámil podle čl. 9 odst. 1, se v prvním členském státě uznávají ode dne použitelnosti prováděcích aktů uvedených v čl. 8 odst. 3 a čl. 12 odst. 8. Dotyčné členské státy informují Komisi. Komise tyto informace zveřejní.

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

V Bruselu dne 23. července 2014.

Za Evropský parlament	*Za Radu*
předseda	*předseda*
M. SCHULZ	S. GOZI

PŘÍLOHA I

POŽADAVKY NA KVALIFIKOVANÉ CERTIFIKÁTY PRO ELEKTRONICKÉ PODPISY

Kvalifikované certifikáty pro elektronické podpisy obsahují:

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

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

— v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,

— v případě fyzické osoby: jméno osoby;

c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů;

e) označení začátku a konce doby platnosti certifikátu;

f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;

g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);

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

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

PŘÍLOHA II

POŽADAVKY NA KVALIFIKOVANÉ PROSTŘEDKY PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ

1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby:

   a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu;

   b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla prakticky vyskytnout pouze jednou;

   c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu nelze odvodit a že elektronický podpis je v současnosti dostupnými technickými prostředky spolehlivě chráněn proti padělání;

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

2. Kvalifikované prostředky pro vytváření elektronických podpisů nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním.

3. Data pro vytváření elektronických podpisů může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru.

4. Aniž je dotčen bod 1 písm. d), smějí kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří spravují data pro vytváření elektronických podpisů jménem podepisující osoby, kopírovat data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky:

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

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

PŘÍLOHA III

POŽADAVKY NA KVALIFIKOVANÉ CERTIFIKÁTY PRO ELEKTRONICKÉ PEČETĚ

Kvalifikované certifikáty pro elektronické pečetě obsahují:

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

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

— v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,

— v případě fyzické osoby: jméno osoby;

c) alespoň jméno pečetící osoby a případné registrační číslo uvedené v úředních záznamech;

d) data pro ověřování platnosti elektronických pečetí, která odpovídají datům pro vytváření elektronických pečetí;

e) označení začátku a konce doby platnosti certifikátu;

f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;

g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);

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

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

PŘÍLOHA IV

POŽADAVKY NA KVALIFIKOVANÉ CERTIFIKÁTY PRO AUTENTIZACI INTERNETOVÝCH STRÁNEK

Kvalifikované certifikáty pro autentizaci internetových stránek obsahují:

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

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

— v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,

— v případě fyzické osoby: jméno osoby;

c) v případě fyzických osob: alespoň jméno osoby, jíž byl certifikát vydán, nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

v případě právnických osob: alespoň název právnické osoby, jíž byl certifikát vydán, a případné registrační číslo uvedené v úředních záznamech;

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

e) název domény nebo domén, které provozuje fyzická nebo 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 služeb vytvářejících důvěru;

h) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;

i) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene h);

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