JOSEF DONÁT, PARTNER ROWAN LEGAL

Revoluce jménem eIDAS

Právní jistota při elektronickém právním jednání – i to je cílem celoevropské úpravy tzv. elektronických identit a služeb.

Jen málo uživatelů elektronického prostředí si uvědomuje, jak zásadním právním předpisem je 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 (dále jen „*eIDAS*"). Nejen že v celém rozsahu nahrazuje dosavadní právní úpravu elektronických podpisů, elektronických značek a souvisejících služeb, které jsou dosud regulovány prostřednictvím zákona č. 227/2000 Sb., o elektronickém podpisu, (dále jen „*ZEP*"), ale nově nastoluje celoevropskou úpravu tzv. elektronických identit a služeb vytvářejících důvěru, což by mělo významně zjednodušit právní jistotu při elektronickém právním jednání. Smyslem tohoto pojednání je poskytnout čtenářům velmi stručný přehled základních aspektů nařízení eIDAS a srovnat jej v základních parametrech s dosavadní právní úpravou. Stručně se dotkneme též nově připravovaného zákona o službách vytvářejících důvěru pro elektronické transakce a o změně některých zákonů (dále jen „*ZSD*"), který nařízení eIDAS doplňuje a upravuje některé specifické aspekty v českém právním prostředí.[1]

Přehled druhů a parametrů elektronických podpisů dle nařízení eIDAS ve srovnání s předchozí právní úpravou

Základní pojetí elektronického podpisu dle ZEP a dle eIDAS

Podle ZEP jsou elektronickým podpisem „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*". ZEP rozlišuje několik druhů elektronických podpisů:

- elektronický podpis bez přívlastků, tj. tzv. „*prostý*" elektronický podpis;
- zaručený elektronický podpis;
- uznávaný elektronický podpis.

Pokud jde o novou úpravu takových podpisů, nařízení eIDAS definuje:

- elektronický podpis bez přívlastků (tj. „*prostý*" elektronický podpis),
- zaručený elektronický podpis, pojmově v zásadě odpovídající zaručenému elektronickému podpisu dle ZEP (viz dále);
- kvalifikovaný elektronický podpis, jímž je zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

Vedle výše popsaných kategorií elektronického podpisu nařízení eIDAS zavádí v ustanovení § 5 návrhu ZSD legislativní zkratku uznávaného elektronického podpisu, pod který se řadí:

- zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy;
- kvalifikovaný elektronický podpis.

Oproti naší úpravě nařízení eIDAS zpřísňuje požadavky na kvalifikovaný elektronický podpis, neboť pro splnění jeho znaků totiž nestačí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy, ale nezbytný je podpis vytvořený kvalifikovaným prostředkem pro

1) V rámci tohoto článku pracujeme s návrhem ZSD ve znění, které bylo přístupné v aplikaci Aplikace ODok v prosinci 2015.

vytváření elektronických podpisů (zpravidla půjde o čipové karty, USB tokeny v kombinaci s požadavkem na zadání PIN při jejich použití apod.).

Prostý elektronický podpis

S prostým elektronickým podpisem podle ZEP nejsou spojené žádné zvláštní náležitosti, a proto se za takový podpis považují údaje, které:

- jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které
- slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.

Přestože ZEP pro zjištění těchto požadavků nestanoví žádné zvláštní podmínky, nařízení eIDAS požadavky na to, co musí (prostý) elektronický podpis splňovat, dále rozvolňuje, když stanoví, že elektronickým podpisem jsou 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.

Zjevně tak odpadá požadavek na jednoznačné určení podepisující osoby, tudíž dosud poněkud sporný charakter např. podpisu v e-mailové zprávě již nyní parametry elektronického podpisu naplňovat bude. Je zřejmé, že takový podpis nebude vhodný pro komunikaci s orgány veřejné moci a bude vhodný spíše pro soukromoprávní komunikaci, kde požadavky na průkaznost nemusí být vysoké, nebo pokud je průkaznost odvoditelná z dalších skutečností, které mohou[2] nebo nemusí[3] přímo souviset se samotným podpisem datové zprávy.

Zaručený elektronický podpis

Podle ZEP je zaručeným elektronickým podpisem podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou – podepisující osoba musí disponovat určitým unikátním znakem, na jehož základě s ní lze podpis jednoznačně spojit;
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě – užitá technologie musí umožnit podepisující osobu jednoznačně identifikovat (obvykle obsahuje elektronický podpis jméno a příjmení, ale může jít i o pseudonym);
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou – podepisující osoba by měla mít pod svou výhradní kontrolou prostředky, kterými i. byl podpis vytvořen, a kterými ii. byl připojen k datové zprávě;
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, který umožňuje zjistit jakoukoliv následnou změnu dat – není tedy nutné zabránit změně dat, ale jde o možnost spolehlivě rozpoznat, pokud by k nějaké změně došlo.[4]

Nařízení eIDAS uvedený přístup s drobnými odchylkami přebírá (zejm. písm. a), b) a d) výše), když odlišně v čl. 26 stanoví, že zaručený elektronický podpis musí být vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou. Z uvedené definice je patrné, že nejde o absolutní kontrolu nad daty pro vytvoření podpisů, ale o požadavek na vysokou úroveň důvěry, tj. adresuje v praxi obvyklé interpretační problémy v otázce absolutního vyloučení třetí strany z kontroly nad prostředky pro vytváření a připojení podpisů k datové zprávě.

Uznávaný elektronický podpis

Podle § 11 ZEP lze k podepisování nebo označování dokumentu v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči státu,[5] použít pouze uznávaný elektronický podpis nebo uznávanou elektronickou značku. Obdobné platí i pro úkony činěné těmito osobami.

> **K podepisování nebo označování dokumentu v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči státu, lze použít pouze uznávaný elektronický podpis nebo uznávanou elektronickou značku.**

Podle ZEP je uznávaným elektronickým podpisem;

- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby anebo
- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie.

Jak je naznačeno výše, podle ZSD do kategorie uznávaného elektronického podpisu patří dva druhy elektronických podpisů, a to:

- zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy;
- kvalifikovaný elektronický podpis.

V návaznosti na nařízení eIDAS stanoví ZSD v § 5, že pokud je elektronickým podpisem podepisován elektronický dokument, jímž se činí úkon vůči státu,[6] lze k tomu použít pouze uznávaný elektronický podpis. Tento požadavek tak podobně, jako dle ZEP, platí i při komunikaci opačným směrem.

Kvalifikovaný elektronický podpis ve smyslu nařízení eIDAS

Jedním ze zásadních přínosů nařízení eIDAS je, že poprvé staví na roveň podpis elektronický a vlastnoruční, a to konkrétně v případě kvalifikovaného elektronického podpisu. Uznávání kvalifikovaného elektronického podpisu ve všech členských státech bude vynucováno do dvou let od začátku povinnosti

2) Příkladem použití prostého elektronického podpisu s vyšší mírou průkaznosti, ale nedosahujícího parametrů zaručeného elektronického podpisu, může být např. biometrický nebo biodynamický podpis spojující datovou zprávu s určitými jedinečnými prvky týkajícími se podepisující osoby.

3) Pokud např. na e-mailovou objednávku podepsanou prostým připojením jména a příjmení odesílatele osoby navazuje faktické plnění, např. úhrada ceny objednaného plnění, je průkaznost jednání podepsaného prostým elektronickým podpisem zvýšena.

4) Viz Peterka, Jiří. Báječný svět elektronického podpisu, str. 68. Praha, 2011. [on-line] [Cit. dne 10. 12. 2015] Dostupné z https://secure.nic.cz/files/bajecny_svet/peterka_bs_cznic.pdf.

5) Ale také dalším institucím, které jsou v pozici veřejné moci, konkrétně územnímu samosprávnému celku, právnické osobě zřízené zákonem, zřízené nebo založené státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem, právnické osobě vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti, či fyzické osobě vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti.

6) Dtto.

na straně veřejného sektoru – do té doby budou moci používat zaručené elektronické podpisy založené na kvalifikovaném certifikátu pro elektronické podpisy bez toho, aby je vytvářeli pomocí kvalifikovaných prostředků.

Přehled druhů a parametrů elektronických značek, elektronických pečetí, časových razítek a dalších nástrojů dle nařízení eIDAS ve srovnání s předchozí právní úpravou

Elektronické značky a elektronické pečetě

ZEP pracuje s pojmy (prosté) elektronické značky a uznávané elektronické značky, které slouží k identifikaci označující osoby (kterou může být i právnická osoba) pomocí kvalifikovaného systémového certifikátu a zajišťují integritu označené datové zprávy. Uznávanou elektronickou značkou je taková značka, která je založena na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Nařízení eIDAS namísto elektronických značek přichází s pojmem tzv. elektronické pečetě, které rozlišuje na „prosté", zaručené a kvalifikované (viz čl. 3 body 25, 26 a 27 nařízení eIDAS). Cílem elektronických pečetí je zaručit původ a integritu dokumentu a dat, k nimž jsou připojeny. Elektronické pečetě nahrazují v nařízení eIDAS elektronické značky založené na systémových certifikátech, ale jak plyne z čl. 3 bodu 29 nařízení eIDAS, na rozdíl od nich jsou nyní dostupné jen pro právnické osoby. Podobně jako došlo k rozšíření kategorie uznávaných elektronických podpisů, je i zde podle ZSD stanoveno, že za uznávané elektronické pečetě se považují:

- zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť;
- kvalifikovaná elektronická pečeť.

Kvalifikovanou elektronickou pečetí podle nařízení eIDAS je zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť, která byla vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí. Co se týče úkonů vůči veřejnému sektoru, popř. jeho používání elektronické pečeti, platí vše, co bylo napsáno u kvalifikovaného elektronického podpisu, přičemž u kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena. Kvalifikovaná elektronická pečeť založená na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaná elektronická pečeť ve všech ostatních členských státech.

Díky přeshraničnímu uznávání prostředků pro elektronickou identifikaci mohou uživatelé se svou „domácí" identitou využít i zahraniční on-line dostupné služby poskytované subjektem veřejného sektoru.

Časová razítka

Podobně jako ZEP, i nařízení eIDAS upravuje použití kvalifikovaného časového razítka, které důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem. Takové kvalifikované časové razítko musí být vydáno kvalifikovaným poskytovatelem certifikačních služeb a nařízení eIDAS rozlišuje časové razítko prosté a kvalifikované splňující dodatečné požadavky (srov. čl. 3 body 33 a 34 nařízení eIDAS), přičemž stejně jako v předchozím případě i zde u kvalifikované formy platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž je toto datum a čas spojeno. Pro uznávání napříč členskými státy platí totéž.

Požadavky na kvalifikovaná elektronická časová razítka jsou podle čl. 42 nařízení eIDAS následující:

- kvalifikované elektronické časové razítko spojuje datum a čas s daty takovým způsobem, aby bylo přiměřeně zamezeno možnosti nezjistitelné změny dat;
- kvalifikované elektronické časové razítko je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem;
- kvalifikované elektronické časové razítko je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.

Nové instituty představené v eIDAS

Certifikáty pro autentizaci internetových stránek

Speciální kategorií zavedenou v rámci nařízení eIDAS je certifikát pro autentizaci internetových stránek, který umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán (viz čl. 3 body 38 a 39). Jedná se o regulaci v praxi již zavedených tzv. SSL certifikátů, přičemž nařízení eIDAS nemá ambice měnit dosavadní stav, ale pouze jej právně aprobovat.[7]

Elektronická identifikace

Novinkou, kterou nařízení eIDAS v kapitole II upravuje, je oblast elektronické identifikace a autentizace. V zásadě je ponecháno na vůli zákonodárce, zda této možnosti využije a zavede prostředky pro účely identifikace, popř. jestli do toho zahrne i soukromý sektor (viz recitál 13 preambule nařízení eIDAS). Na druhou stranu však nařízení eIDAS stanovuje povinnost přeshraničního uznávání, tudíž i když se členský stát nerozhodne využít prostředky elektronické identifikace, bude jejich užívání nucen za určitých okolností uznat. Samotné uznávání je postaveno na bázi národních identitních uzlů a jejich komunikace přes společné rozhraní. Jako klíčová schémata elektronické identifikace budou dle aktuálních informací zavedeny elektronické občanské průkazy s čipem, které budou od 1. 1. 2017 vydávány občanům zdarma.

Díky přeshraničnímu uznávání prostředků pro elektronickou identifikaci používaných v jednotlivých systémech elektronické identifikace mohou uživatelé se svou *„domácí"* identitou využít i zahraniční on-line dostupné služby poskytované subjektem veřejného sektoru a nemusí k tomu u zahraničního poskytovatele služeb zařizovat uživatelský účet, resp. samostatnou identitu – proto pokud se např. občan Estonska bude chtít přihlásit do internetového portálu některého z českých úřadů, bude muset Česká republika zajistit, že se bude schopen přihlásit

7) Viz Průša, J. Evropa má novou legislativu: ovlivní e-podpis, datové schránky i serverové certifikáty. [online] [Cit. dne 10. 12. 2015] Dostupné z https://blog.nic.cz/2014/08/29/evropa-ma-novou-legislativu-ovlivni-e-podpis-datove-schranky-i-serverove-certifikaty/.

prostřednictvím své národní elektronické identity (v tomto případě prostřednictvím elektronického občanského průkazu Estonska).

Úrovně záruky systémů elektronické identifikace:

Nařízení eIDAS stanoví v čl. 8 pro systémy elektronické identifikace celkem tři úrovně záruky tohoto systému: nízkou, značnou nebo vysokou s rozdílnými stupni spolehlivosti, přičemž minimální technické specifikace, normy a postupy stanoví prováděcí akt k nařízení eIDAS.

Z hlediska bezpečnosti a ochrany před zneužitím údajů v rámci systémů elektronické identifikace je důležité stanovení odpovědnosti;

- členského státu, který oznámil Evropské komisi daný systém elektronické identifikace a úmyslně či z nedbalosti nesplnil své povinnosti plynoucí z nařízení eIDAS;
- strany vydávající prostředky pro elektronickou identifikaci, která při tom úmyslně či z nedbalosti porušila povinnosti plynoucí z nařízení eIDAS;
- strany provozující postup autentizace, která úmyslně či z nedbalosti nezajistí správné fungování autentizace za škodu způsobenou fyzické či právnické osobě. Tato odpovědnost vyplývá z čl. 11 nařízení eIDAS.

Služby vytvářející důvěru

Třetím pilířem nařízení eIDAS je institut služeb vytvářejících důvěru. Službou vytvářející důvěru se rozumí elektronická služba, která je zpravidla poskytována za úplatu a spočívá:

- 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
- ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo
- v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami.[8]

Účelem institutu služeb vytvářejících důvěru je posílení důvěry občanů a organizací v Evropské unii v elektronické transakce. Proto je stanoveno, že by mělo „*být možné použít je ve všech členských státech jako důkaz v soudním a správním řízení.*“[9] Samotné nařízení však nestanoví vyčerpávajícím způsobem, jaké jsou účinky služeb vytvářejících důvěru a vnitrostátnímu právu členských států je dána možnost vymezit právní účinky služeb vytvářejících důvěru, pokud to samotné nařízení v určité otázce nevylučuje.[10]

Účinky služeb vytvářejících důvěru jsou stanoveny pro jednotlivé služby odlišně. Obecně však nařízení stanoví, že pokud nějakému subjektu „*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.*“[11] Zároveň nařízení stanoví, že „*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.*“[12] Z tohoto ustanovení lze dovozovat, že pokud veřejný subjekt (např. správní orgán či soud) nebude, např. z ekonomických důvodů, disponovat vybavením nezbytným pro technickou čitelnost určité služby vytvářející důvěru, bude stále povinen ji uznávat a nesmí jí upřít účinky, protože ji nedokáže přečíst nebo ověřit.

> **Třetím pilířem nařízení eIDAS je institut služeb vytvářejících důvěru.**

Služby vytvářející důvěru podle nařízení eIDAS se opět dělí na služby „*prosté*“ a služby kvalifikované. Kategorie kvalifikovaných služeb vytvářejících důvěru a kvalifikovaných poskytovatelů služeb vytvářejících důvěru byly vytvořeny „*za účelem stanovení požadavků a povinností, které zajistí vysokou úroveň bezpečnosti všech používaných nebo poskytovaných kvalifikovaných služeb vytvářejících důvěru a produktů.*“[13] Pro poskytovatele kvalifikovaných služeb jsou stanoveny přísnější požadavky v oblasti odpovědnosti, zabezpečení a nutného dohledu.

8) Článek 3 bod. 16 nařízení eIDAS.
9) Recitál 22 nařízení eIDAS.
10) Tamtéž.
11) Recitál 23 nařízení eIDAS.
12) Tamtéž.
13) Recitál 28 nařízení eIDAS.

Odpovědnost za škodu:
První otázka, která je ve vztahu ke službám vytvářejícím důvěru v nařízení eIDAS upravena, je otázka odpovědnosti za škodu a důkazního břemena. V zásadě lze říci, že poskytovatelé těchto služeb odpovídají za škodu způsobenou fyzické či právnické osobě, a to jak úmyslně či z nedbalosti, jednáním (i nejednáním) poskytovatele v rozporu s nařízením.[14] Z důvodu změkčení této tvrdosti pak nařízení eIDAS zavádí povinnost uzavření pojistné smlouvy a další omezení, kdy se takové odpovědnosti poskytovatel potenciálně zprostí.[15]

V případě vzniku škody českým poskytovatelem služeb vytvářejících důvěru se povinnost bude řídit primárně § 2894 a násl. o. z. V případě, že by služba vytvářející důvěru byla provozována ze strany státu, přednostně by se odpovědnost řídila zákonem č. 82/1998 Sb., o odpovědnosti státu za škodu způsobenou při výkonu veřejné moci, ve znění pozdějších předpisů. Problematické v praxi bude rozlišení, který právní předpis na konkrétní situaci bude dopadat, protože si lze již teď představit hypotetické situace, kdy aplikace toho kterého předpisu bude přinejmenším sporná.

Rozdílně pak nařízení eIDAS upravuje otázku důkazního břemene, přičemž půjde-li o škodu vzniklou nekvalifikovaným poskytovatelem, bude důkazní břemeno na tom, kdo tento nárok uplatňuje – v případě kvalifikovaného poskytovatele ponese důkazní břemeno právě tento poskytovatel.[16]

Bezpečnostní opatření:
Za účelem prevence škod nařízení eIDAS dále ukládá poskytovatelům služeb vytvářejících důvěru povinnost přijmout „*vhodná technická a organizační opatření k řízení rizik ohrožujících bezpečnost jimi poskytovaných služeb vytvářejících důvěru*,"[17] přičemž tato opatření musí zajišťovat úroveň bezpečnosti, která je přiměřená míře rizika s ohledem na nejnovější technologický vývoj, „*zejména musí být přijata opatření k zabránění bezpečnostním incidentům, k minimalizaci jejich dopadů a k informování zúčastněných stran o nepříznivých dopadech těchto incidentů.*"[18]

Součástí povinností poskytovatelů tak bude sledovat technologický vývoj, monitorovat rizika a podle toho dbát na zvolená bezpečnostní opatření, přičemž esenciální opatření nutné pro všechny poskytovatele stanoví Evropská komise prováděcím aktem.[19]

Pro kvalifikované poskytovatele služeb vytvářejících důvěru jsou pak některé konkrétnější požadavky stanoveny přímo nařízením eIDAS.

Další důležitou povinností poskytovatele služeb vytvářejících důvěru je povinnost oznamovat bezpečnostní incidenty, které jsou vymezeny jako narušení bezpečnosti nebo ztráta integrity, jež má významný dopad na poskytovanou službu vytvářející důvěru nebo na uchovávané osobní údaje. O bezpečnostních incidentech jsou všichni poskytovatelé služeb vytvářejících důvěru (jak kvalifikovaní, tak nekvalifikovaní) povinni vyrozumět orgán dohledu a případné další příslušné subjekty, jako jsou příslušný vnitrostátní orgán pro bezpečnost informací nebo orgán pro ochranu údajů. V prostředí České republiky tak poskytovatelé budou povinni vyrozumět také Úřad pro ochranu osobních údajů a Národní bezpečnostní úřad.[20] Toto oznámení se vztahuje i na zákazníky poskytovatele, kterých by se incident mohl dotknout; z toho důvodu musí být bezodkladně informováni, popř. takovou povinnost může nařídit orgán dohledu.[21]

Nad veškerými poskytovateli služeb vytvářejících důvěru bude v rámci jejich působení na trhu Evropské unie vykonáván dohled. Pro Českou republiku bude dohledovým orgánem ministerstvo vnitra.

Dohled státních orgánů:
Nad veškerými poskytovateli služeb vytvářejících důvěru bude v rámci jejich působení na trhu Evropské unie vykonáván dohled[22] a každý členský stát je povinen k tomuto účelu určit orgán dohledu na svém území, přičemž pro Českou republiku bude tímto orgánem ministerstvo vnitra.[23]

Příslušný orgán dohledu bude vykonávat svoje povinnosti vůči těm poskytovatelům služeb vytvářejících důvěru, kteří budou usazeni na území příslušného členského státu bez ohledu na to, na jakých trzích v rámci Evropské unie budou tito poskytovatelé působit.[24] Nařízení eIDAS tak prakticky implementuje tzv. princip *one-stop-shop*, kdy je poskytovatel pro celý trh Evropské unie povinen jednat primárně s jedním dohledovým orgánem, který bude s ostatními spolupracovat[25] (typicky u přeshraničně působících poskytovatelů služeb vytvářejících důvěru).[26]

◆◆◆

Vzhledem k omezenému rozsahu tohoto článku bylo cílem alespoň stručným způsobem nastínit čtenářům základní instituty nového nařízení eIDAS a srovnat jej s dosavadní právní úpravou, nicméně komplexita tohoto právního předpisu a jeho potenciální dopady do života občanů vyžadují celou řadu navazujících detailních pojednání o jednotlivých dílčích aspektech, jako je například implementace elektronických občanských průkazů, vztah mezi nařízením eIDAS a datovými schránkami, možné využití služeb vytvářejících důvěru z pohledu podnikatelů či uživatelů anebo faktické změny ve způsobu využívání elektronických podpisů dle nařízení eIDAS v praxi. ◆

14) Článek 13 odst. 1 nařízení eIDAS.
15) Recitál 37 nařízení eIDAS.
16) Článek 13 odst. 1 nařízení eIDAS.
17) Článek 19 odst. 1 nařízení eIDAS.
18) Tamtéž.
19) Článek 19 odst. 3 písm. a) nařízení eIDAS.
20) Článek 19 odst. 2 nařízení eIDAS.
21) Článek 19 odst. 2 nařízení eIDAS. Dle českého překladu nařízení může orgán dohledu o zveřejnění poskytovatele „požádat", v souladu s anglickým zněním se však domníváme, že úmyslem evropského zákonodárce bylo umožnit orgánu dohledu zveřejnění požadovat („require").
22) Článek 17 odst. 1 nařízení eIDAS.
23) Přinejmenším to vyplývá z § 9 odst. 1 ZSD.
24) Článek 17 odst. 2 písm. a) a b) nařízení eIDAS.
25) Článek 18 nařízení eIDAS.
26) Recitál 42 nařízení eIDAS.