



Datové schránky, elektronický podpis a autorizovaná konverze dokumentů



doc. JUDr. Ing. BOHUMÍR
ŠTĚDRŮN, Ph.D., LL.M., MBA



Mgr. JOSEF PROKEŠ

1. PRÁVNÍ ÚPRAVA

Institut datových schránek a autorizované konverze dokumentů zavedl do českého právního řádu zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále jen „zákon“). Zákon nabyl účinnost dnem 1. července 2009 pro autorizovanou konverzi a s odkladným účinkem pro některé právníké profese ohledně povinnosti si nechat zřídit datovou schránku.

2. DATOVÉ SCHRÁNKY

Datová schránka je elektronické úložiště, které je určeno k (i.) doručování orgány veřejné moci, (ii.) provádění úkonů vůči orgánům veřejné moci, a (iii.) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Datové schránky zřizuje a spravuje ministerstvo vnitra.

POUŽITÍ DATOVÝCH SCHRÁNEK

- **povinně**
 - obousměrná komunikace orgánů veřejné moci mezi sebou
 - komunikace orgánů veřejné moci vůči některým právnickým osobám
 - komunikace orgánů veřejné moci vůči právnickým nebo fyzickým osobám, které si datovou schránku zřídily dobrovolně nebo jim byla zřízena na základě zákona
- **nepovinně**
 - komunikace fyzických osob vůči orgánům veřejné moci
 - komunikace podnikajících osob mezi sebou za jistých okolností

- **předmětem úvah je širší využití datových schránek pro neomezenou komunikaci mezi fyzickými a právnickými osobami**

Všeckrá komunikace v oblasti veřejné správy má probíhat elektronicky, pokud je to z povahy věci možné. V případě orgánů veřejné moci je za účelem snížení ekonomických nákladů stanoveno povinné použití elektronické formy komunikace. Pokud má fyzická či právnická osoba zřízení datovou schránku, musí orgán veřejné moci doručovat v elektronické formě právě do datové schránky dané osoby. K přístupu do jedné datové schránky však může být oprávněno více osob. Všechny osoby nemusí mít přístup ke všem datovým zprávám, které jsou ve schránce. To je významné pro institut doručování do vlastních rukou adresáta, pak taková datová zpráva není ostatním oprávněným osobám přístupná.

Informační systém datových schránek je uzavřeným systémem, který obsahuje datové schránky, metadata o uživateli a jejich oprávněních a o datových zprávách, které jsou prostřednictvím tohoto systému „zasílány“ (fyzicky k žádnému faktickému zaslání nedochází, zpráva je uložena na serveru v datové schránce, dokud ji z této schránky adresát nevybere). V principu se jedná o informační systém postavený nad databází, se kterým je možné komunikovat prostřednictvím grafického uživatelského rozhraní, a rozhraní poskytující webové služby jiným informačním systémům. Nejde tedy o klasický e-mailový systém, kde jsou zprávy posílány z jednoho serveru na druhý. Systém umožňuje také přeposlání zprávy na e-mail (jako přílohu), např. na adresu elektronické podatelny.

ID DATOVÉ SCHRÁNKY JAKO OSOBNÍ ÚDAJ

K bezpečnému používání datové schránky stanoví zákon pro uživatele dva základní postupy:

- obezřetné zacházení s přístupovými údaji (§ 9 zákona)
- zneplatnění přístupových údajů v mimořádném případě na základě oznámení (§ 12 zákona)

Informace o komunikaci s datovou schránkou, obsah přenášených zpráv i zacházení s přístupovými údaji, byť by se jednalo o datovou schránku právnické osoby, jsou přiřaditelné ke konkrétní oprávněné fyzické osobě a již z tohoto důvodu je třeba dodržovat povinnosti požadované zákonem č. 101/2000 Sb., o ochraně osobních údajů.

ID datové schránky je kódem – osobním údajem,¹ který vypovídá

- o statutu osoby (oprávnění k datové schránce)
- o jednání oprávněné osoby (v konkrétním případě zacházení s datovou schránkou)

¹ Definice viz § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů.

Vedle přihlašovacích údajů je v mechanismu datových schránek nutno stejným způsobem nahlížet na každou informaci o procesu či události, které vyžadují lidský zásah nebo mají sebemenší vliv na lidské jednání. Takové informace jsou podřaditelné pod skupinu údajů osobní povahy, podléhajících zákonné ochraně, neboť na jejich základě jsou jednotlivci alespoň nepřímo identifikovatelní.²

3. DEFINICE POJMU A DRUHY AUTORIZOVANÝCH KONVERZÍ

Zákon definuje autorizovanou konverzi (dále jen „konverze“) jako (i.) *úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky*, nebo (ii.) *úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky*. **Platí důležitá zákonná zásada, že dokument, který provedením konverze vznikl (zákon označuje jako „výstup“), má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl (zákon označuje jako „vstup“).**³ Zákon dále dodává, že má-li být podle jiného právního předpisu předložen dokument v listinné podobě správnímu orgánu, nebo soudu anebo jinému státnímu orgánu, zejména aby byl užit jako podklad pro vydání rozhodnutí, je tato povinnost splněna předložením jeho výstupu. Tímto ustanovením zákon zakotvuje povinnost pro veřejné orgány přijímat konverze (výstupy).

KONVERZE JE TEDY MOŽNÉ ROZDĚLIT DLE HLEDISKA:

- **předmětu konverze**
 - listinný dokument se konvertuje do elektronického dokumentu (datové zprávy)
 - datová zpráva se konvertuje do listinného dokumentu
- **orgánů, který konverzi provádí**
 - konverze na žádost (Jedná se o službu, kterou vedle advokátů poskytují např. Czech POINTy nebo notáři.)
 - konverze z moci úřední (Konverze z moci úřední slouží pro vnitřní potřeby úřadu. Všechny orgány veřejné moci si mohou konvertovat dokumenty pro výkon své působnosti.)

4. SUBJEKTY OPRAVNĚNÉ KONVERZI PROVÁDĚT

Zákon stanoví, že konverzi na žádost provádějí kontaktní místa veřejné správy⁴ a konverzi z moci úřední provádějí orgány veřejné moci pro výkon své působnosti. Dále jsou konverzi oprávněni provádět notáři, exekutoři a nedávno tuto možnost získali i advokáti.

5. POSTUP PŘI PROVÁDĚNÍ KONVERZE

Při konverzi do dokumentu v listinné podobě subjekt provádějící konverzi nejdříve⁵

- a) ověří platnost kvalifikovaného časového razítka⁶ vstupu, je-li jím vstup opatřen,
- b) ověří, že kvalifikovaný certifikát⁷ vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je

založen zaručený elektronický podpis, kterým je podepsán vstup, nebo kvalifikovaný systémový certifikát vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založena elektronická značka, kterou je označen vstup, nebyly před okamžikem uvedeným v kvalifikovaném časovém razítku zneplatněny,

- c) ověří platnost zaručeného elektronického podpisu⁸ založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo platnost uznávané elektronické značky.⁹

Bezodkladně poté, kdy subjekt provádějící konverzi ověří shodu výstupu se vstupem a shoduje-li se výstup se vstupem, připojí k výstupu ověřovací doložku.

Při konverzi do dokumentu obsaženého v datové zprávě opatří subjekt, který konverzi provedl, výstup svou uznávanou elektronickou značkou nebo uznávaným elektronickým podpisem osoby, která konverzi provedla, a zajistí, aby byl výstup opatřen kvalifikovaným časovým razítkem.

Technické parametry ke konverzi specifikuje vyhláška č. 193/2009, o stanovení podrobností provádění autorizované konverze dokumentů.¹⁰

Při konvertování dokumentů je nutné identifikovat a zaznamenat bezpečnostní prvky, kterými se dokument před převedením vyznačoval (např. vodoznak), sloužící jednak k jeho ochraně proti pozměňování (ochrana integrity dokumentu), jednak k ochraně práv jeho autora. Přítomnost bezpečnostních prvků v dokumentu se volí před vlastním zahájením konverze. Některé speciální bezpečnostní prvky však (zatím) konvertovat nelze (pečetě).

6. CO NELZE KONVERTOVAT

Zákon výslovně stanoví, že **konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy.**

Vstup v listinné podobě nesmí být ve stavu způsobilém poškodit snímací zařízení nebo ve stavu způsobilém přivodit provedením konverze své poškození. Vstup obsažený v datové zprávě nesmí obsahovat škodlivý kód, který je způsobilý přivodit škodu na informačním systému subjektu provádějícího konverzi nebo na informacích zpracovávaných subjektem provádějícím konverzi.

2 Obecně platí, že číslo každé věci, i komunikačního prostředku, dokládá statut či jednání člověka, který jej používá. Z tohoto důvodu je tudíž na takové číslo pohlíženo jako na osobní údaj. Blíže viz stanovisko evropské skupiny pro ochranu údajů (WP 29), č. 4/2007 k pojmu osobní údaje, ze dne 20. 6. 2007.

3 § 22 odst. 2 zákona.

4 Podrobněji viz zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

5 § 24 zákona.

6 Viz zákon č. 227/2000 Sb., o elektronickém podpisu (ZoEP). Vysvětleno v další části článku (Elektronický podpis, certifikát a elektronická značka).

7 Viz zákon č. 227/2000 Sb., o elektronickém podpisu (ZoEP). Vysvětleno v další části článku (Elektronický podpis, certifikát a elektronická značka).

8 Viz zákon č. 227/2000 Sb., o elektronickém podpisu (ZoEP). Vysvětleno v další části článku (Elektronický podpis, certifikát a elektronická značka).

9 Viz zákon č. 227/2000 Sb., o elektronickém podpisu (ZoEP). Vysvětleno v další části článku (Elektronický podpis, certifikát a elektronická značka).

10 Více informací na www.czechpoint.cz v sekci „konverze dokumentů“.

ZÁKON DÁLE NEUMOŽŇUJE PROVÁDĚT KONVERZI V TĚCHTO PŘÍPADECH:¹¹

- je-li dokument v jiné než v listinné podobě či v podobě datové zprávy,
- jde-li o dokument v listinné podobě, jehož jedinečnost nelze konverzí nahradit, zejména o občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los, sázenku, geometrický plán, rysy a technické kresby,
- jsou-li v dokumentu v listinné podobě změny, doplňky, vsuvky nebo škrty, které by mohly zeslabit jeho věrohodnost,
- není-li z dokumentu v listinné podobě patrné, zda se jedná o
 1. prvopis,
 2. vidimovaný dokument,
 3. opis nebo kopii pořízenou ze spisu, nebo
 4. stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle jiného právního předpisu,
- je-li dokument v listinné podobě opatřen plastickým textem nebo otiskem plastického razítka,
- v případě provedení konverze na žádost, nebyl-li dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil,
- jde-li o dokument obsažený v datové zprávě, který nelze konvertovat do listinné podoby, například o zvukový nebo audiovizuální záznam,
- pokud dokument nesplňuje technické náležitosti stanovené vyhláškou č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů.

7. ELEKTRONICKÝ PODPIS, ELEKTRONICKÝ CERTIFIKÁT, ELEKTRONICKÁ ZNAČKA A ČASOVÉ RAZÍTKO

Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. Zákonná definice v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu (dále „ZoEP“) zní, že *elektronický podpis jsou 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.*

Elektronický podpis tedy zajišťuje:

- **Ověření integrity zprávy** – příjemce má jistotu, že zpráva nebyla změněna v průběhu transportu (např. v prostředí internetu).

- **Zaručuje nepopiratelnost zprávy** – odesílatel nemůže popřít, že danou zprávu s daným obsahem opravdu odeslal.
- **Nenapodobitelnost podpisu** – prostředky k podpisování může mít daná osoba pod svou výhradní kontrolou.

ZOEP ROZEZNÁVÁ TŘI DRUHY ELEKTRONICKÉHO PODPISU

• Prostý elektronický podpis¹²

Jedná se o údaje v elektronické podobě, které jsou připojeny k datové zprávě nebo jsou s ní logicky spojeny a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. Může jít tedy teoreticky i o ruční podpis, který je naskenovaný a vložen do textu e-mailu.

• Zaručený elektronický podpis¹³

Splňuje definice prostého elektronického podpisu (e-podpis), ale s tou odlišností, že třetí nestranná a důvěryhodná osoba se „zaručuje“, že e-podpis patří opravdu vám, a to tak, že vám vydá nástroje pro vytváření a ověřování elektronického podpisu (jedná se o software pro vytváření e-podpisu). Tato třetí osoba se nazývá **certifikační autorita** a potvrzení o tom, že vy jste vlastníkem e-podpisu, se nazývá **elektronický certifikát**.

• Uznávaný elektronický podpis¹⁴

Splňuje všechny znaky zaručeného elektronického podpisu s tím rozdílem, že nestranná třetí strana – certifikační autorita musí mít akreditaci od státu (povolení), aby mohla vydávat software k tvorbě elektronického podpisu. Tato třetí strana se potom nazývá **akreditovaná certifikační autorita** a někdy se přirovnává k jakémusi „elektronickému“ notáři.¹⁵ **Důležité je, že pouze uznávaný elektronický podpis je možné používat při komunikaci s veřejnou správou.**

Elektronická značka¹⁶ (elektronické razítko) je z technického hlediska totéž jako elektronický podpis s tím rozdílem, že zatímco e-podpis je určen pro fyzické osoby jako jejich projev vůle, tak elektronická značka je určena především pro právnické osoby, elektronické značky mohou být tedy vytvářeny – generovány automaticky softwarem.

Časové razítko důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala v daný časový okamžik. Časové razítko je služba poskytovaná certifikační autoritou, která umožňuje prokázat čas vytvoření dokumentu. Samotný elektronický podpis prokazuje identitu tvůrce, ale neumožňuje dokázat, že je čas vytvoření dokumentu správný. Pro odstranění tohoto nedostatku bylo vytvořeno časové razítko.

✦ Prvý autor, advokát, je soudním znalcem pro informační technologie a auditor ICT, druhý autor je ředitel odboru legislativy a zahraničních vztahů Úřadu pro ochranu osobních údajů.

11 § 24 odst. 5 zákona.

12 § 2 písm. a) ZoEP.

13 § 2 písm. b) ZoEP.

14 § 11 ZoEP.

15 V ČR mají akreditaci tyto tři certifikační autority: 1) PostSignum (www.postsignum.cz), 2) 1. certifikační autorita a. s. (www.ica.cz) a 3) eidentity (www.eidentity.cz).

16 § 2 písm. c) ZoEP.