

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Shrnutí stanoviska evropského inspektora ochrany údajů ke sdělení Komise nazvanému „Uvolnění potenciálu cloud computingu v Evropě“

(Úplné znění tohoto stanoviska naleznete v angličtině, francouzštině a němčině na stránkách evropského inspektora ochrany údajů na adrese <http://www.edps.europa.eu>)

(2013/C 253/03)

I. Úvod

I.1 Cíl stanoviska

1. S ohledem na důležitost cloud computingu v rozvíjející se informační společnosti a na pokračující politickou diskusi v rámci EU o cloud computingu se evropský inspektor ochrany údajů rozhodl vydat z vlastního podnětu toto stanovisko.

2. Toto stanovisko je odpovědí na sdělení Komise ze dne 27. září 2012 nazvané „Uvolnění potenciálu cloud computingu“ (dále jen „sdělení“) ⁽¹⁾, které stanovuje klíčová opatření a politické kroky, jež je třeba podniknout, má-li být urychleno používání služeb cloud computingu v Evropě. Před přijetím sdělení proběhla neformální konzultace s evropským inspektorem ochrany údajů, který vznesl neformální připomínky. Vítá, že některé z jeho připomínek byly ve sdělení zohledněny.

3. Vzhledem k rozsahu a důležitosti probíhající diskuse o vztahu mezi cloud computingem a právním rámcem pro ochranu údajů se toto stanovisko nicméně neomezuje pouze na témata, kterými se zabývá sdělení.

4. Stanovisko se zaměřuje zejména na problémy, které cloud computing představuje z hlediska ochrany údajů, a na to, jak by je vyřešilo navrhované nařízení o ochraně údajů (dále jen „navrhované nařízení“) ⁽²⁾. Vyjadřuje se rovněž k oblastem, ve kterých je podle sdělení třeba podniknout další opatření.

I.2 Souvislosti

5. V souvislosti s obecnou politickou diskusí v EU o cloud computingu mají zvláštní význam následující činnosti a dokumenty:

- Komise po svém sdělení z roku 2010 nazvaném „Digitální program pro Evropu“ ⁽³⁾ zahájila veřejné konzultace o cloud computingu v Evropě, které probíhaly od 16. května do 31. srpna 2011, a výsledky zveřejnila dne 5. prosince 2011 ⁽⁴⁾,
- Dne 1. července 2012 přijala pracovní skupina zřízená podle článku 29 ⁽⁵⁾ stanovisko ke cloud computingu (dále jen „stanovisko PS29“) ⁽⁶⁾, které analyzuje uplatňování současných pravidel pro ochranu údajů, jež stanovila směrnice 95/46/ES, na poskytovatele služeb v oblasti cloud computingu působících v Evropském hospodářském prostoru (EHP) a jejich zákazníky ⁽⁷⁾,
- Dne 26. října 2012 přijali komisaři pro ochranu údajů a soukromí během své 34. mezinárodní konference usnesení o cloud computingu ⁽⁸⁾.

⁽¹⁾ COM(2012) 529 final.

⁽²⁾ COM(2012) 11 final.

⁽³⁾ KOM(2010) 245 final.

⁽⁴⁾ http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

⁽⁵⁾ Pracovní skupina zřízená podle článku 29 je poradním orgánem, který byl zřízen podle článku 29 směrnice 95/46/ES. Tvoří ji zástupci vnitrostátních orgánů dozoru, evropský inspektor ochrany údajů a zástupce Komise.

⁽⁶⁾ Stanovisko WP29 č. 05/2012 ke cloud computingu, k dispozici na adrese: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_cs.pdf

⁽⁷⁾ Kromě toho vnitrostátní orgány pro ochranu údajů v několika členských státech vydaly na vnitrostátní úrovni své vlastní pokyny pro cloud computing, např. v Itálii, Švédsku, Dánsku, Německu, Francii a Spojeném království.

⁽⁸⁾ Usnesení o cloud computingu přijaté během 34. mezinárodní konference komisařů pro ochranu údajů konané v Uruguayi, dne 26. října 2012.

I.3 Sdělení o cloud computingu

6. Evropský inspektor ochrany údajů sdělení vítá. Následující tři opatření, která jsou označována jako specifická a klíčová, jsou na úrovni EU požadována za účelem doplnění a podpory používání cloud computingu v Evropě:

- klíčové opatření č. 1: radikální řešení nepřehledné situace v oblasti norem,
- klíčové opatření č. 2: zajištění bezpečných a spravedlivých smluvních podmínek,
- klíčové opatření č. 3: vytvoření evropského partnerství pro cloud computing na podporu inovací a růstu ze strany veřejného sektoru.

7. Předjímají se rovněž další politické kroky, jako jsou opatření motivující k využívání cloud computingu pomocí podpory výzkumu a vývoje či zlepšování informovanosti nebo nezbytnost řešit klíčová témata týkající se služeb cloud computingu (zahrnující mimo jiné ochranu údajů, přístup k údajům za účelem prosazování práva, bezpečnost, odpovědnost zprostředkujících poskytovatelů služeb) prostřednictvím posíleného mezinárodního dialogu.

8. Ochrana údajů je ve sdělení zmíněna jako zásadní prvek pro zajištění úspěšného zavedení cloud computingu v Evropě. Sdělení konstatuje ⁽¹⁾, že navrhované nařízení se zabývá mnohými z obav, jež nadnesli poskytovatelé služeb cloud computingu a zákazníci využívající služeb cloud computingu ⁽²⁾.

I.4 Zaměření stanoviska a jeho struktura

9. Toto stanovisko má tři cíle.

10. Prvním cílem je upozornit v rámci současných diskusí o cloud computingu na význam soukromí a ochrany údajů. Stanovisko zejména zdůrazňuje, že úroveň ochrany údajů v prostředí cloud computingu nesmí být nižší než úroveň požadovaná v jakémkoli jiném kontextu zpracování údajů. Postupy týkající se cloud computingu se mohou rozvinout a zákonně uplatňovat pouze tehdy, pokud zaručí dodržení této úrovně ochrany údajů (viz kapitolu III.3). Stanovisko zohledňuje pokyny obsažené ve stanovisku PS29.

11. Druhým cílem je podrobněji rozebrat hlavní problémy, které cloud computing přináší pro oblast ochrany údajů, v souvislosti s navrhovaným nařízením o ochraně údajů, zejména obtíže spojené s jednoznačným stanovením odpovědnosti jednotlivých aktérů a pojmů správce a zpracovatel. Stanovisko (zejména kapitola IV) rozebírá, jak by navrhované nařízení v současné podobě ⁽³⁾ pomohlo zajistit vysokou úroveň ochrany údajů v oblasti služeb cloud computingu. Vychází tedy z názorů, které evropský inspektor ochrany údajů rozvinul ve svém stanovisku k balíčku opatření pro reformu ochrany údajů (dále jen „stanovisko evropského inspektora ochrany údajů k balíčku opatření pro reformu ochrany údajů“) ⁽⁴⁾, a doplňuje ho zvláštním zohledněním prostředí cloud computingu. Evropský inspektor ochrany údajů zdůrazňuje, že jeho stanovisko k balíčku opatření pro reformu ochrany údajů se v plné míře týká i služeb cloud computingu a je třeba ho brát jako základ pro současné stanovisko. Některé otázky zmiňované ve stanovisku k balíčku opatření (např. analýza nových ustanovení ohledně práv subjektu údajů) ⁽⁵⁾ jsou navíc dostatečně jasné a nebudou tedy v současném stanovisku dále rozvíjeny.

12. Třetím cílem je určit oblasti, které s ohledem na strategii cloud computingu předloženou ve sdělení Komise vyžadují další opatření na úrovni EU z hlediska ochrany údajů a soukromí. Patří mezi ně mimo jiné poskytnutí dalších pokynů, snahy o normalizaci, provedení dalších posouzení rizik pro konkrétní odvětví (jako je veřejný sektor), vytvoření standardních smluvních podmínek, zapojení se do mezinárodního dialogu o otázkách týkajících se cloud computingu a zajištění účinných prostředků mezinárodní spolupráce (budou vypracovány v kapitole V).

⁽¹⁾ Viz strana 8 sdělení, oddíl „Opatření digitální agendy pro vytváření digitální důvěry“.

⁽²⁾ Pojmem „zákazníci využívající služeb cloud computingu“ se v tomto stanovisku obecně označují jak zákazníci jednající jako podniky, tak spotřebitelé jednající jako jednotliví koncoví uživatelé.

⁽³⁾ Je třeba vzít v úvahu, že návrh nařízení v současné době řádným legislativním postupem projednává Rada a Evropský parlament.

⁽⁴⁾ Stanovisko je k dispozici na adrese: <http://www.edps.europa.eu>

⁽⁵⁾ Viz stanovisko evropského inspektora ochrany údajů, zejména odst. 140 až 158.

13. Stanovisko má tuto strukturu: Oddíl II poskytuje přehled hlavních znaků cloud computingu a souvisejících problémů ohledně ochrany údajů. Oddíl III přezkoumává nejdůležitější prvky stávajícího právního rámce EU a navrhovaného nařízení. Oddíl IV rozebírá, jak by navrhované nařízení pomohlo řešit problémy spojené s ochranou údajů, které vyvolalo používání služeb cloud computingu. Oddíl V rozebírá návrhy Komise na další vývoj politiky a určuje oblasti, kde může být zapotřebí vyvinout další úsilí. Oddíl VI obsahuje závěry.

14. Zatímco řada připomínek tohoto stanoviska se vztahuje na všechna prostředí, ve kterých se používá cloud computing, stanovisko se nezabývá využíváním služeb cloud computingu konkrétně orgány a institucemi EU, které podléhají dohledu evropského inspektora ochrany údajů podle nařízení (ES) č. 45/2001. Pokyny k tomuto tématu vydá pro zmíněné orgány a instituce evropský inspektor ochrany údajů samostatně.

VI. Závěry

121. Jak popisuje sdělení, cloud computing nabízí řadu nových příležitostí pro podniky, spotřebitele a veřejný sektor, pokud jde o správu údajů prostřednictvím použití vzdálených externích zdrojů IT. Současně představuje mnoho výzev, zejména ohledně příslušné úrovně ochrany, kterou tento způsob zpracovávání zajišťuje dotčeným údajům.

122. Hlavní riziko, které s sebou nese používání služeb cloud computingu, představuje postupná ztráta odpovědnosti, která souvisí se zpracováním údajů poskytovateli služeb cloud computingu, a to pokud nejsou kritéria použitelnosti právních předpisů EU v oblasti ochrany údajů dostatečně jasná a pokud je úloha a odpovědnost poskytovatelů služeb cloud computingu definována nebo chápána v příliš omezeném rozsahu nebo není účinně uplatňována. Evropský inspektor ochrany údajů zdůrazňuje, že používání služeb cloud computingu nemůže ospravedlnit zmírnění norem pro ochranu údajů oproti normám platným pro obvyklé postupy zpracování údajů.

123. V tomto ohledu by navrhované nařízení o ochraně údajů tak, jak bylo předloženo, mnohé aspekty vyjasnilo a přineslo by řadu nástrojů, které by pomohly zajistit, že poskytovatelé služeb nabízející služby zákazníkům usídleným v Evropě dodržují uspokojivou úroveň ochrany údajů. Jde zejména o následující:

- článek 3 by vyjasnil územní působnost pravidel EU pro ochranu údajů a rozšířil by jejich rozsah i na služby cloud computingu,
- čl. 4 bod 5 by zavedl nový prvek správcovství, kterým jsou „podmínky“; to by bylo v souladu s vývojovým trendem, podle kterého je s ohledem na technickou složitost informačních technologií, které tvoří základ pro poskytování služeb cloud computingu, nezbytné rozšířit okolnosti, za kterých je možné považovat poskytovatele služeb cloud computingu za správce. To by lépe odráželo skutečnou míru vlivu na zpracování,
- navrhované nařízení by zvýšilo odpovědnost správců údajů a zpracovatelů údajů tím, že by zavedlo konkrétní povinnosti, jako je ochrana údajů již od návrhu a standardní nastavení ochrany údajů (článek 23), ohlašování případů narušení bezpečnosti údajů (článek 31 a 32) a posuzování dopadu na ochranu údajů (článek 33). Dále by vyžadovalo, aby správci a zpracovatelé údajů zavedli mechanismy pro ověření účinnosti uskutečněných opatření na ochranu údajů (článek 22),
- články 42 a 43 navrhovaného nařízení by umožnily pružněji používat mezinárodní mechanismy předávání údajů, aby zákazníci a poskytovatelé služeb cloud computingu mohli snáze přijmout vhodné záruky pro ochranu údajů při předávání osobních údajů datovým centřům nebo serverům umístěným ve třetích zemích,
- články 30, 31 a 32 navrhovaného nařízení by objasnily povinnosti správců a zpracovatelů ohledně bezpečnosti zpracovávání a požadavků na informace v případě narušení bezpečnosti údajů; tím by položily základ komplexnímu a kooperativnímu přístupu k řízení bezpečnosti uplatňovanému mezi jednotlivými aktéry v prostředí cloud computingu,

- články 55 až 63 navrhovaného nařízení by posílily spolupráci orgánů dozoru a jejich koordinovaný dozor nad přeshraničním zpracováváním, což je zvláště důležité v prostředí, jako je cloud computing.

124. Po zohlednění specifík služeb cloud computingu evropský inspektor ochrany údajů nicméně navrhuje, aby se v navrhovaném nařízení blíže objasnily následující aspekty:

- pokud jde o územní působnost navrhovaného nařízení, čl. 3 odst. 2 písm. a) by měl znít „s nabídkou zboží nebo služeb zahrnujících zpracování osobních údajů těchto subjektů údajů v Unii“, nebo by měl být přidán nový bod odůvodnění, který upřesní, že zpracovávání osobních údajů subjektů údajů v EU ze strany správců, kteří nejsou usazeni v EU a kteří poskytují služby právnickým osobám usazeným v EU, také spadá do územní působnosti navrhovaného nařízení,
- jak evropský inspektor ochrany údajů uvádí ve svém stanovisku k balíčku opatření pro reformu ochrany údajů, měla by být přidána jasná definice pojmu „předávání“,
- mělo by být přidáno zvláštní ustanovení, které by objasnilo podmínky, za kterých je možné povolit přístup k údajům uchovávaným ve službách cloud computingu orgánům pověřeným prosazováním zákonů ze zemí mimo EHP. Součástí takového ustanovení může být též povinnost příjemce žádosti informovat a konzultovat v konkrétních případech příslušný orgán dozoru v EU.

125. Evropský inspektor ochrany údajů rovněž zdůrazňuje, že bude zapotřebí dalších pokynů ze strany Komise nebo orgánů dozoru (zejména prostřednictvím budoucí Evropské rady pro ochranu údajů), pokud jde o následující aspekty:

- vyjasnění toho, které mechanismy by se měly zavést, aby se zajistilo ověřování účinnosti opatření na ochranu údajů v praxi,
- pomoc zpracovatelům s používáním závazných podnikových pravidel a s dosahováním souladu s příslušnými požadavky,
- poskytnutí osvědčených postupů pro otázky, jako je odpovědnost správců/zpracovatelů, náležité uchování údajů v prostředí cloud computingu, přenositelnost údajů a výkon práv subjektů údajů.

126. Evropský inspektor ochrany údajů dále uznává, že užitečným nástrojem, který by posílil soulad a rovněž důvěru mezi různými subjekty, by mohly být kodexy chování vytvořené odvětvím a schválené příslušnými orgány dozoru.

127. Evropský inspektor ochrany údajů podporuje myšlenku, aby Komise na základě konzultace s orgány dozoru vytvořila standardní smluvní podmínky pro poskytování služeb cloud computingu, jež budou dodržovat požadavky na ochranu údajů, zejména pak:

- vypracování modelových smluvních podmínek, které budou zahrnuty v obchodních podmínkách nabídek služeb cloud computingu,
- vypracování společných podmínek a požadavků pro zadávání zakázek ve veřejném sektoru, přičemž se zohlední citlivost zpracovávaných údajů,
- přizpůsobení mezinárodních mechanismů pro předávání údajů v prostředí cloud computingu, zejména prostřednictvím aktualizace současných standardních smluvních doložek a navržení standardních smluvních doložek pro předávání údajů zpracovatelům usazeným mimo EU ze strany zpracovatelů usazených v EU.

128. Evropský inspektor ochrany údajů upozorňuje, že požadavky na ochranu údajů bude nutné náležitě zvážit při vytváření norem a certifikačních systémů, přičemž se jedná zejména o:

- uplatnění zásad ochrany soukromí již od návrhu a standardního nastavení ochrany soukromí při vytváření norem,
- začlenění požadavků na ochranu soukromí, jako jsou omezení týkající se účelu a uchovávání, do návrhu norem,
- povinnost poskytovatelů poskytnout svým zákazníkům informace nezbytné k provedení platného posouzení rizik a informace o bezpečnostních opatřeních, která provedli, a také o ohlašování bezpečnostních incidentů.

129. Evropský inspektor ochrany údajů nakonec zdůrazňuje, že problémy, které přináší cloud computing, je nezbytné řešit na mezinárodní úrovni. Vybízí Komisi, aby se zapojila do mezinárodního dialogu o otázkách, jež spolu s cloud computingem vyvstaly, včetně otázek spojených s jurisdikcí a přístupem k údajům na základě prosazování práva, a navrhuje, že řadu z těchto otázek by bylo možné vyřešit různými mezinárodními nebo dvoustrannými dohodami, jako jsou dohody o vzájemné pomoci a také obchodní dohody. Na mezinárodní úrovni by měly být vytvořeny celosvětové normy, které by stanovily minimální podmínky a zásady pro přístup k údajům ze strany donucovacích orgánů. Je rovněž zastáncem toho, aby orgány dozoru vypracovaly účinné mezinárodní mechanismy spolupráce, zvláště ve vztahu k problematice cloud computingu.

V Bruselu dne 16. listopadu 2012.

Peter HUSTINX
evropský inspektor ochrany údajů
