DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

5. 2. 2024

Informace pro vývojářské firmy a jejich řešení formulářových podání v rámci zákona č. 12/2020 Sb., o právu na digitální služby

Úvod

Zákon č. 12/2020 Sb., o právu na digitální služby (dále jen „ZoPDS“) zavádí právo občanů činit digitální úkon vůči orgánům veřejné moci (dále jen „OVM“). Ustanovení § 4 odst. (3) vysloveně ukládá OVM zveřejňovat elektronické formuláře, které za podmínek stanovených ZoPDS umožní učinit digitální úkon, a to (zjednodušeně) prostřednictvím datové schránky, elektronickým dokumentem s připojeným uznávaným elektronickým podpisem, nebo interaktivně přes webové rozhraní (portálové řešení) – dle volby uživatele služby.

Řešení, která se pro OVM na trhu připravují, mohou využívat výhody cloudových služeb. Zejména jde o to, že využívání elektronických služeb pro veřejnost a jejich kapacitní nároky bude zpočátku obtížné odhadnout. Dodavatelské firmy proto budou muset zajistit rychlou škálovatelnost výpočetního výkonu a současně odpovídající úroveň zabezpečení.

Povinnosti, vyplývající ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „ZoISVS“)

V souvislosti s možným využitím cloudových služeb upozorňujeme OVM, které jsou současně i orgány veřejné správy (dále jen „OVS“)[1], resp. správci informačního systému veřejné správy (dále jen „ISVS")[2], i jejich možné dodavatele (ve smyslu poskytovatele cloud computingu – dále jen „poskytovatele CC“) – na následující pravidla a povinnosti vyplývající z využívání CC[3]:

1) **Zhodnocení, na jaké architektonické úrovni je využíván cloud computing** (dále jen „CC“)
   S ohledem na definici CC v ZoISVS § 2 odst. (2) písm. b) je třeba vyhodnotit:
   a) Jestli dané řešení využívá **plně dedikovanou instanci aplikačního softwaru**, který si dané OVM samostatně instaluje ve svém cloudovém tenantu – pak se jedná o **CC třídy IaaS a příp. PaaS.** Dále uvedené regulatorní požadavky se uplatní jen pro třídy IaaS/PaaS a jejich poskytovatele.
   b) V případě, že se jedná o **instanci aplikačního softwaru sdílenou mezi více OVM** a administrovanou centrálně nějakým poskytovatelem CC, jedná se o **CC třídy SaaS**. Dále uvedené regulatorní požadavky se uplatní pro třídy IaaS, PaaS i SaaS a jejich poskytovatele.

   Z metodického hlediska lze uvést, že cloudový model SaaS zde bude pro OVM pravděpodobně finančně výhodnější, protože je může méně zatěžovat po stránce systémové administrace a může lépe zefektivnit využití výpočetních zdrojů použité platformy.
2) **Poskytovatel CC musí být zapsán do katalogu CC** dle požadavků ZoISVS.
3) **Poptávaný CC pro dané řešení již musí být zapsán jako nabídka CC v katalogu CC** dle požadavků ZoISVS, a to v rozsahu, v jakém se skutečně jedná o CC (viz body 1 a) a 1 b) výše)

[1] Upozorňujeme, že ZoPDS se vztahuje na OVM, zatímco ZoISVS se vztahuje na OVS.

[2] ve smyslu ZoISVS

[3] viz Hlava VI ZoISVS

4) **Správce ISVS musí zařadit poptávaný CC do příslušné bezpečnostní úrovně** (dále jen „BÚ")[4] dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (dále jen „vyhl. č. 315/2021").

   Zde přichází v úvahu důležitý moment, a to je možné uplatnění **dekompozice front-endové části řešení ISVS** (dle § 4 ZoPDS) pro jednotlivá podání do nižší bezpečnostní úrovně v souladu s § 4 odst. (2) vyhl. č. 315/2021.

   Je-li tedy např. ISVS jako celek zařazen do BÚ 3 nebo i do BÚ 4, může přesto správce ISVS vyhodnotit maximální možné dopady kybernetického bezpečnostního incidentu na front-endové části jako nižší, a rozhodnout o její dekompozici do nižší BÚ než vykazuje např. centrální back-end ISVS a jeho úložiště agregovaných dat.

   Podle tabulky úrovní a oblastí dopadů (příloha k vyhl. č. 315/2021) lze očekávat, že funkce pořizování strukturovaných údajů autentizovaných uživatelů pomocí jednotlivých formulářů, jejich dočasné uložení a automatizované odeslání do back-endové části ISVS v mnoha případech nenaplní úroveň dopadu v žádné z oblastí A až I pro úroveň vyšší než je „2. Střední". Klíčovou oblastí posuzování dopadů přitom může být oblast B. – Ochrana osobních údajů. Z vodítka uvedeného pod tabulkou vyplývá, že pro úroveň dopadu „2. Střední" je možné naplnit tři a více kritérií z první skupiny uvedených kritérií, avšak nesmí dojít k naplnění více než jednoho kritéria z druhé skupiny uvedených kritérií, které zahrnují (zjednodušeně):

   a) zpracování zvláštních kategorií osobních údajů atd. (viz výčet) **=> *toto může nastat dle typu zpracovávaných dat v daném ISVS***.

   b) zpracování osobních údajů více než 10.000 subjektů údajů ***=> pravděpodobně nenastane.*** *Dotčení vyššího počtu subjektů údajů může nastat v případě, kdy front-endové řešení bude muset z důvodu nedostupnosti back-endové části ISVS data ukládat na dobu až několika dní. Správce ISVS musí provést kvalifikovaný odhad maximálního objemu podání v dočasném úložišti a případně může i zvýšit dobu dostupnosti svého back-endu na 24x7, příp. 12x7 atd.*

   c) automatizované rozhodování, které se dotýká subjektů údajů ***=> pravděpodobně nenastane*** *v rámci funkčnosti front-endové části ISVS.*

   Toto předpokládané vyhodnocení úrovní dopadů směřuje k **zařazení, případně k dekompozici front-endových formulářových řešení do BÚ 2.**

   Naopak pro možnou dekompozici front-endové části do nejnižší úrovně dopadu „1. Nízká" musí správce ISVS řádně vyhodnotit zejména oblasti F. – Řízení a provoz, G. – Důvěryhodnost, I. – Zajišťování služeb, kde může v mnoha případech nastat překročení této „nízké" úrovně dopadu, což by opět mohlo směřovat k výslednému vyhodnocení úrovně dopadu jako „2. Střední".

   Správce ISVS musí samozřejmě zohlednit i jiné možné dopady ztráty důvěrnosti, integrity nebo dostupnosti dat zpracovávaných ve front-endové části – tedy i mimo oblast B. – Ochrana osobních údajů, pokud takové dopady neosobních dat přichází v úvahu v případě daného ISVS.

   Nutnou podmínkou dekompozice formulářové front-endové části řešení do nižší BÚ je rovněž taková architektura, která znemožní útočníkovi případnou kompromitací front-endové části získat přístup i k centrální databázi back-endové části.

[4] BÚ 1 – Nízká, BÚ 2 – Střední, BÚ 3 – Vysoká, BÚ 4 – Kritická

V mnoha případech lze tedy očekávat, že správci ISVS budou poptávat funkčnost formulářových řešení jakožto části svých (jednoho nebo více) ISVS, **zařazených** (a případně dekomponovaných) **do BÚ 2.** Okrajově však nelze vyloučit ani zařazení do BÚ 3 nebo BÚ 1.

Vodítka pro vývojářské firmy (dále jen „ISV“[5]), které chtějí nabízet správcům ISVS[6] formulářová řešení pro splnění požadavků ZoPDS s využitím CC

Poskytovatel CC i jeho služby CC musí být zapsány v katalogu CC (viz body 2 a 3 výše).

Podmínkou zápisu služeb CC (tj. tzv. nabídky cloud computingu dle ZoISVS) do katalogu CC je splnění kritérií uvedených ve vyhl. č. 316/2021 Sb. o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhl. č. 316/2021“), a to v rozsahu, který se uplatní pro danou BÚ a pro příslušný rozsah odpovědnosti daného ISV:

a) Jestliže bude daný ISV provozovat nabízené řešení formou SaaS na vlastní platformě IaaS/PaaS, musí splnit podmínky zápisu v určené BÚ všemi architektonickými vrstvami IaaS, PaaS i SaaS.

b) Jestliže bude daný ISV provozovat nabízené řešení formou SaaS na platformě IaaS/PaaS jiného poskytovatele, musí být zapsán i tento poskytovatel podpůrného CC a v určené BÚ také ten podpůrný CC, využívaný daným ISV.

Z hlediska nutných certifikací a auditních zpráv, které si musí daný ISV zajistit pro prokázání splnění požadavků uvedených ve vyhl. č. 316/2021 pro zápis nabídky CC do katalogu CC (dle ZoISVS), se mohou jevit jako nejnáročnější:

- **pro BÚ 2**: certifikace **ISO/IEC 27001** v rozsahu kontrolních bodů zahrnujících i **ISO/IEC 27017**. Tuto certifikaci není možné obejít jiným způsobem pro ID 8.2 a ID 8.4 (viz vyhl. č. 316/2021)
- **pro BÚ 3**: certifikace **ISO/IEC 27001** v rozsahu kontrolních bodů zahrnujících i **ISO/IEC 27017** a dále **ISO/IEC 27018** – opět nutné pro ID 6.5, 8.3, 8.5, 8.6. Navíc je zde ID 8.7, které vyžaduje také auditní zprávu **SOC2 Type 2** (viz další podrobnosti ve vyhl. č. 316/2021), a to i pro poskytovatele cloudových služeb SaaS.

Vzhledem ke skutečnosti, že ISVS zařazené do BÚ 3 jsou zpravidla významnými informačními systémy dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“) s vysokou úrovní dopadů dle vyhl. č. 315/2021, je třeba zajistit audit služeb CC v BÚ 3 a v BÚ 4 dostatečně důvěryhodným způsobem.

Další povinnosti správců ISVS a poskytovatelů CC jakožto zpracovatelů osobních údajů vyplývající z obecného nařízení GDPR

V případě jakéhokoli zpracování osobních údajů se poskytovatel CC (i pouhé vrstvy SaaS) pravděpodobně stane i „zpracovatelem“ dle nařízení GDPR. V takovém případě bude nutná úroveň zabezpečení zpracovávaných dat u front-endové části určena také (kromě požadavků ze ZoISVS a ZoKB) výsledkem posouzení rizik pro práva a svobody subjektů osobních údajů podle GDPR. Správce osobních údajů (zde zpravidla i správce ISVS) musí se zpracovatelem osobních údajů uzavřít tzv. zpracovatelskou smlouvu podle čl. 28 GDPR.

[5] Independent Software Vendor (ISV)

[6] Budou-li poskytovatelé nabízet cloudová řešení OVM, které nejsou současně OVS, případně OVS avšak mimo rozsah vymezení ISVS v rámci ZoISVS, zde uvedené povinnosti se na ně neuplatní.

S ohledem na maximální požadovanou dobu dočasného uložení formulářových dat a úroveň citlivosti těchto dat musí správce ISVS s pomocí zpracovatele společně zvolit adekvátní úroveň zabezpečení takového dočasného úložiště, kde může dojít (byť dočasně) k jisté agregaci vstupních dat.

Lze očekávat, že situace (i) zpracování pouhých základních identifikačních osobních údajů, a současně (ii) kontext podání, který nepředstavuje vysoká rizika pro subjekty údajů, a současně (iii) místo dočasného uložení osobních údajů v datových centrech v zemích Evropského hospodářského prostoru, případně s předáním založeným na rozhodnutí o odpovídající ochraně[7], nebudou vyžadovat šifrování osobních údajů v úložišti. Správce ISVS pak může vyžadovat jen zabezpečení řízením přístupu k dočasnému úložišti, případně takové šifrování v úložišti, které je pod kontrolou poskytovatele CC.

Avšak v ostatních případech, kdy se může jednat o zpracování s vysokým rizikem pro práva a svobody subjektů údajů (byť jen několika subjektů – fyzických osob), bude na základě posouzení vlivu na ochranu osobních údajů (DPIA)[8] pravděpodobně vyžadováno využití šifrování dat v dočasném úložišti. Pokud se bude jednat o cloudové úložiště s místem uložení dat mimo země Evropského hospodářského prostoru, měly by být šifrovací klíče pod plnou kontrolou správce ISVS, tedy minimálně s využitím varianty kombinace HSM[9] modulu v cloudu a technologie BYOK[10].

Bližší instrukce a vodítka k problematice posouzení vlivu na ochranu osobních údajů poskytuje publikace ÚOOÚ[11] „Metodika obecného posouzení vlivu na ochranu osobních údajů“ a dále „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů“.

Závěr

ISV v roli poskytovatele CC při nabízení formulářových front-endových řešení pro OVS musí být nejprve zapsán v katalogu CC jako poskytovatel, a dále musí být zapsána jeho služba SaaS, a současně musí být zapsané i využívané služby cloudové platformy IaaS/PaaS, a to způsobem, který poskytuje adekvátní míru zabezpečení s ohledem na charakter zpracování (včetně požadavků GDPR). Z tržního hlediska mohou ISV očekávat, že velká část poptávaných řešení ze strany OVS bude zařazena do BÚ 2.

[7] předání osobních údajů podle čl. 45 GDPR

[8] Data Protection Impact Assessment (DPIA)

[9] Hardware Security Module (HSM)

[10] Bring Your Own Key (BYOK)

[11] https://uoou.gov.cz/profesional/metodiky-a-doporuceni-pro-spravce/posouzeni-vlivu-na-ochranu-osobnich-udaju