SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

V PRAZE DNE 8. DUBNA 2022

Stanovisko Svazu průmyslu a dopravy České republiky k návrhu nařízení Evropského parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (Data Act)

Svaz průmyslu a dopravy ČR (dále jen SPČR) dlouhodobě prosazuje, aby se sdílení dat v EU řídilo především principy dobrovolnosti. Evropská komise (dále jen EK) dne 23. února 2022 zveřejnila návrh Nařízení Evropského parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (dále jen Data Act), který dle vyjádření EK přináší nová pravidla ohledně toho, kdo může mít napříč hospodářskými odvětvími přístup k datům generovaným v EU a využívat je. SPČR návrh nařízení Data Act obecně vítá, protože má potenciál usnadnit toky dat a souhlasí i s principem více práv pro spotřebitele, tzn. přístup ke svým datům a jejich sdílení. Je však potřeba nastavit systém, který bude funkční a napříč celým návrhem se vyskytuje řada nejasností, které bude potřeba v průběhu projednávání vyřešit.

Podrobněji k jednotlivým oblastem v návrhu:

Působnost: Vítáme vymezení působnosti nařízení na držitele a příjemce dat získaných prostřednictvím IoT zařízení, výrobce IoT zařízení, veřejný sektor a poskytovatele služby zpracování dat. Oblast působnosti však není zcela jasně vymezena. Umožňuje proto intepretace, dle kterých by měly některé části nařízení (zejm. kapitola V – Zpřístupňování dat subjektům veřejného sektoru a institucím, agenturám nebo orgánům Unie na základě výjimečné potřeby) dopadnout na držitele všech typů dat. Působnost nařízení a jednotlivé definice, zejm. definice pojmu „data holder“ by měly být zpřesněny, aby poskytovaly dostatečnou právní jistotu povinným subjektům. Dále jde např. o zahrnutí chytrých televizorů a hlasových asistentů, ovšem s výjimkou stolních počítačů nebo chytrých telefonů, které přitom mají tendenci plnit v mnoha případech podobné funkce a mají přístup ke stejným službám. Definice „related services“ je rovněž nejasná, protože neřeší vymezení odpovědnosti mezi zúčastněnými stranami dodavatelského řetězce, které mají nejlepší pozici pro poskytování přístupu k datům. Pojem “generated data” je nutné specifikovat – vyskytuje se napříč návrhem a není součástí definic.

Sdílení dat B2B: Koncept by měl být opravdu jasně definován. Jak bychom např. měli rozumět pojmu „data holder"? Považuje se za držitele dat také vývojář softwaru, který software prodává svým zákazníkům, kteří jej následně implementují do zařízení IoT? Domníváme se, že by tomu tak nemělo být (stejně jako vývojář AI pro obecné účely, na kterého by se neměly vztahovat požadavky AI Act).

Povinnosti třetích stran přijímajících data: Subjekty přijímající data je nesmí používat k vývoji konkurenčních služeb. Protože ale v návrhu není žádná definice, není jasné, jak by se vůbec dozvěděly o konkurenčních službách držitele dat. Ani to, jak by se tento bod vynucoval. Celkově vzato, jakmile jsou data sdílena s třetí

TELEFON (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

ČLEN BUSINESSEUROPE

stranou, není jasné, jak by držitel dat mohl kontrolovat jejich další využití, a jaké strany k nim mohou dále přistupovat.

Právo sdílet data se třetími stranami: Během projednávání bude potřeba sledovat návrh článku 5, protože přenáší koncept gatekeepera z Digital Markets Act (DMA). Zatím se nejedná o dokončenou a platnou legislativu, proto bude potřeba zajistit správnou provázanost obou legislativních návrhů (tento princip lze uplatnit napříč celým návrhem). Dle návrhu společnost označená jako gatekeeper podle DMA není oprávněna přijímat žádná uživatelská data ani v případě souhlasu uživatelů a nesmí pobízet své zákazníky, aby jim svá data přenášeli; tato omezení se vztahují na celou společnost a její služby, nikoliv jen na hlavní služby platformy. Sdílení dat se třetími stranami se pak vztahuje také na produkty, jako jsou např. automobily, a z návrhu není jasné, jak to bude v této oblasti realizováno, aby nedošlo k ohrožení bezpečnosti.

Ochrana obchodního tajemství: Návrh stanovuje podmínky ohledně ochrany obchodních tajemství, pokud nějaká část bude součástí předávaných dat. Neuvádí však, jak by byly chráněny oprávněné zájmy držitelů dat v případě nezákonného použití třetími stranami. Bude nezbytné to specifikovat. Návrh dále obsahuje neurčité pojmy jako např. all necessary measures, který nelze považovat za dostatečně specifikovaný pro zajištění ochrany obchodního tajemství.

Podmínky pro zpřístupnění dat příjemcům: Návrh v článku 8 zavádí nepřiměřenou zátěž pro držitele dat, kteří budou muset prokázat, že podmínky pro zpřístupnění dat nejsou diskriminační. Tuto žádost bude moci příjemce dat podat kdykoliv, pokud bude podmínky za diskriminační „považovat“. Není jasné, proč je příjemcům dat přiznáno právo vznášet paušální obvinění, aniž by své argumenty podložili.

Zpřístupnění dat veřejným orgánům: I když návrh umožňuje veřejným orgánům získávat data v případě, že je to „výjimečně potřeba“, nezahrnuje žádné záruky pro držitele dat, kteří je veřejným orgánům zpřístupňují. Dále bude nezbytné vyjasnit pojem exceptional need, který je definován příliš široce. Za velmi problematická považujeme také ustanovení v článku 17 týkající se pokut za nevyhovění žádosti a pak ustanovení v článku 20, že v případě tzv. public emergency bude poskytnutí dat zdarma. Vůbec nejsou zohledněny náklady výrobců, na které je kladena nová povinnost.

Cloud Switching: Považujeme za zcela legitimní, že Data Act má ambice usnadnit zákazníkům proces přenosu dat a v podstatě tak zajistit, že nenastane tzv. vendor lock-in. Pokus o srovnání cloud switchingu s relativně přímou migrací uložených dat nebo s bezplatnou přenositelností podle GDPR neodráží realitu a rozmanitost cloudových služeb, objem a složitost dat, sdílenou odpovědnost mezi poskytovateli cloudu a zákazníky, potřebu odborné technické pomoci a projektového řízení. Je to velmi rigidní přístup, který bude potřeba vyřešit. Navíc se zdá, že se tyto povinnosti překrývají s povinnostmi týkajícími se přenositelnosti podle DMA. Rovněž je potřeba ověřit, jestli jsou reálné lhůty v článcích 23 a 24.

Mezinárodní přístup a transfer: Navrhované požadavky by mohly vést k faktickým požadavkům na lokalizaci dat a diskriminaci poskytovatelů cloudových služeb legálně usazených v Evropě, na které se mohou vztahovat zákony v jiné jurisdikci, které by mohly být v rozporu s právem EU, avšak bez právního přezkumu. To by mohlo ovlivnit četné a velké toky dat. Bylo by na místě, aby byl k dispozici seznam zemí, se kterými má EU relevantní dohody, jak je uvedeno v článku 27, aby bylo jasné, jak moc problematické toto ustanovení může být.

Interoperabilita: Návrh zmocňuje Komisi k přijímání norem, u nichž se předpokládá soulad s ustanoveními Data Act o interoperabilitě. To považujeme za významnou oblast návrhu, protože zároveň byla zveřejněna

nová Standardization Strategy a počítá se s přezkumem nařízení EU 1025/2012 o evropské normalizaci, na které se Data Act odkazuje. V návrhu se zároveň počítá s oslovením pouze relevantních evropských standardizačních organizací. Nikde v textu není zmíněno, že je potřeba vycházet z již existujících mezinárodních standardů. Obáváme se, aby na základě tohoto přístupu nedošlo ke znevýhodnění ne-evropských firem v přístupu na trh.

Vymáhání: Není jasné, proč je vymáhání, včetně ukládání pokut za nedodržení, rozděleno mezi různé regulační orgány a ponecháno na jednotlivých členských státech. Decentralizovaný systém, který dává členským státům volnost při prosazování pravidel, by mohl vést k různým praktikám v EU. Není jasné, jestli je tento přístup v souladu s cílem vytvořit harmonizovaný právní rámec podle článku 114 SFEU.

Řešení sporů: Návrh stanovuje mechanismus řešení sporů, kterým ale není dotčeno právo stran požádat o účinný opravný prostředek např. u vnitrostátního soudu. Není jasné, jak by to fungovalo v praxi, protože to společnosti vystavuje riziku, že budou mít jeden spor na více fórech a zároveň se tak spor může dlouhodobě protahovat.

Pokuty: Vzhledem k tomu, že návrh stanovuje řadu nových povinností, které dosud fungovaly na principech dobrovolnosti, a zároveň je uvedeno, že v případě tzv. public emergency, má být zpřístupnění dat veřejným orgánům poskytnuto zdarma, považujeme výši pokut, které mají být stanoveny podle ustanovení GDPR, za nepřijatelnou.

Vstup v platnost a použitelnost: Je potřeba přezkoumat, jestli je lhůta 12 měsíců po vstupu v platnost, reálná např. vzhledem k množství nových povinností nebo požadavkům na interoperabilitu.