3. 2. 2025

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Data Governance Act a Data Act (Akt o správě dat a Nařízení o datech) – co obsahují a jaké novinky do oblasti správy údajů tyto nové předpisy přinášejí?

Data Governance Act, tedy Nařízení 2022/868 o evropské správě dat a o změně nařízení (EU) 2018/172, česky často označované jako Akt o správě dat (dále jen „DGA“)[1] je mezisektorový nástroj, jež nabyl účinnosti 24. září 2023 a jehož cílem je regulovat opakované používání veřejně dostupných/chráněných údajů prostřednictvím podpory sdílení údajů napříč sektory, regulace nových zprostředkovatelů dat a podpory sdílení údajů pro altruistické účely.

Do působnosti DGA spadá široké spektrum údajů, a to jak údaje osobní, tak neosobní – nicméně v rozsahu, v jakém se jedná o osobní údaje podle GDPR [2] , se primárně uplatní GDPR a DGA pouze subsidiárně. [3]

Opětovné použití určitých kategorií údajů ve správě orgánů veřejného sektoru

DGA vytváří rámec pro opětovné využití určitých kategorií chráněných dat, která má ve své dispozici veřejný sektor. Zatímco směrnice o otevřených datech[4] upravuje opakované použití veřejně dostupných informací, DGA se zaměřuje na chráněná data, jako jsou osobní a obchodně důvěrné informace, které nelze zveřejnit jako otevřená data. DGA stanoví pravidla a ochranné mechanismy, aby bylo možné tato data znovu využít, pokud to umožňuje jiná legislativa.

V praxi to znamená, že pro to, aby data mohla být poskytnuta, musí být členské státy technicky vybaveny tomu, aby zajistily ochranu soukromí a důvěrnosti dat prostřednictvím anonymizace, pseudonymizace[5] či zabezpečeného zpracovatelského prostředí. Pokud veřejný orgán nemůže data sám poskytnout, měl by žadateli pomoci se získáním souhlasu jednotlivců nebo povolení od držitelů práv. Použití smluv omezujících opětovné využití dat by mělo být podle DGA omezeno na případy veřejného zájmu.

DGA také stanoví, že ač mohou veřejné instituce účtovat přiměřené poplatky, měl by být podporován výzkum a nekomerční účely tím, že poplatky budou sníženy nebo zcela vyloučeny. Žádost o opětovné použití musí být vyřízena do dvou měsíců. Členské státy vytvoří jednotná informační místa a registr

chráněných údajů (ERPD)[6], aby se zjednodušil přístup k těmto informacím v celé EU.

Služby zprostředkovaní údajů

DGA stanovuje pravidla pro poskytovatele zprostředkovatelských služeb dat (tzv. datové zprostředkovatele), kteří fungují jako důvěryhodní organizátoři sdílení dat. Cílem těchto ustanovení je zvýšit důvěru ve sdílení dat prostřednictvím neutrálních a transparentních zprostředkovatelů, aby jednotlivci i podnikatelé měli o nejvyšší kontrolu nad svými daty.

V praxi fungují zprostředkovatelé jako neutrální třetí strany, které propojují ty, kdo data mají, s těmi, kdo je potřebují, aniž by data využívali k vlastnímu finančnímu prospěchu. DGA vyžaduje, aby tyto služby zprostředkování dat byly právně a ekonomicky oddělené od jiných komerčních aktivit a zakazuje zprostředkovatelům profitovat z přímých transakcí s daty nebo z jejich využití k vývoji vlastních produktů. Všechna získaná data mohou být použita pouze ke zlepšení samotných zprostředkovatelských služeb.

Datoví zprostředkovatelé musí oznámit svůj záměr poskytovat zprostředkovatelské služby příslušným úřadům, které ověří jejich soulad s pravidly a následně jim udělí oficiální značku „uznaného poskytovatele zprostředkovatelských služeb EU“ a společné logo. Centrální registr uznaných zprostředkovatelů vede Evropská komise.[7]

Datový altruismus

Datový altruismus umožňuje jednotlivcům a podnikatelům dobrovolně a bez odměny zpřístupnit data pro účely veřejného zájmu, například pro výzkum nebo vývoj lepších produktů a služeb v oblastech jako zdravotnictví, životní prostředí či mobilita. Přestože existuje zájem o datový altruismus, v praxi ho brzdí nedostatek nástrojů pro sdílení dat. Cílem DGA je proto vytvořit důvěryhodné nástroje, které usnadní sdílení dat, a nastavit podmínky zajišťující, že tato data budou zpracována v souladu s hodnotami EU.

Organizace dobrovolně poskytující data se mohou registrovat jako „organizace datového altruismu uznané v EU,“ přičemž musí být neziskové a splňovat požadavky na transparentnost a ochranu práv dárců údajů. Evropská komise s těmito organizacemi spolupracuje na vytvoření příruček obsahujících technické požadavky a bezpečnostní standardy

Evropský sbor pro datové inovace a mezinárodní toky dat

DGA zřizuje Evropskou radu pro datové inovace (EDIB) s cílem sdílet osvědčené postupy v oblastech datového zprostředkování, datového altruismu a využití veřejných údajů, které nelze zpřístupnit jako otevřená data. EDIB sdružuje zástupce členských států, Evropskou komisi, Evropskou agenturu pro kybernetickou bezpečnost (ENISA) a další relevantní odborníky a má za úkol navrhovat pokyny pro společné evropské datové prostory.

DGA dále podporuje mezinárodní datové toky a posiluje strategickou autonomii EU v globálním prostředí. V kontextu neosobních údajů zavádí podobné ochranné mechanismy jako GDPR, které chrání údaje před neoprávněnými žádostmi vlád třetích zemí. Tato ochranná opatření vyžadují, aby

tzv. „reuseři“[8] mimo EU zajistili stejnou úroveň ochrany jako v rámci EU a přijali jurisdikci EU. Pokud je to nutné, může Evropská komise přijmout rozhodnutí o odpovídající ochraně pro přenos chráněných veřejných údajů a vypracovat vzorové smluvní doložky, které zajistí datové přenosy s veřejným sektorem do třetích zemí.

Data Act - základní vymezení a důležité informace

Data Act, tedy Nařízení 2023/2854 Evropského parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828, česky označované též jako Akt o datech nebo Nařízení o datech (dále též „**NOD**“) vstoupilo v platnost 11. ledna 2024 a účinnosti nabude 12. září 2025 – na rozdíl od DGA tedy ještě v účinnosti není.[9] Samotné NOD je klíčovým pilířem Evropské strategie pro data Evropské komise, mimo jiné doplňuje Akt o správě dat a významně přispívá k cíli tzv. Digitální dekády Evropy.[10] Jde tedy o právní předpis, jehož cílem je posílit datové hospodářství Evropské unie a podpořit konkurenceschopný trh s daty prostřednictvím účinnějšího přístupu k údajům (zejména průmyslovým) a jejich využívání. NOD by mělo zvýšit dostupnost dat a tím podpořit inovace založené na datech. NOD totiž podporuje spravedlivé rozdělení hodnoty dat mezi účastníky datové ekonomiky a jasně vymezuje, kdo je oprávněn data používat a za jakých podmínek. Řeší vztahy v oblasti držení a sdílení údajů mezi soukromými subjekty, spotřebiteli a veřejným sektorem.[11] Zjednodušeně řečeno, NOD také definuje, které údaje generované občany státu mohou nebo dokonce musí být sdíleny s podniky a sociálními úřady.[12] Stejně jako u DGA u NOD platí, že se NOD neuplatní na data v rozsahu, v jakém se uplatní GDPR.

V posledních letech došlo na evropském trhu k rychlému nárůstu dostupnosti výrobků připojených k internetu (dále jen „propojené produkty“), přičemž tyto produkty, které dohromady tvoří síť známou jako „internet věcí“ (IoT)[13], výrazně zvyšují rozsah opakovaně použitelných údajů v EU. Právě z důvodu tohoto všeobecného rozšíření či rozmachu internetu věcí NOD umožní spravedlivé rozdělení hodnoty údajů tím, že stanoví jasná a spravedlivá pravidla pro přístup k údajům a jejich využívání v evropském datovém hospodářství.

NOD dále obsahuje opatření, jež by mělo zvýšit spravedlnost a konkurenceschopnost cloudových služeb na evropském trhu, na ochranu společností před nespravedlivými smluvními podmínkami a sdílením údajů, které si nárokují silnější hráči na trhu. Zavádí také mechanismus, jehož prostřednictvím mohou instituce veřejného sektoru požadovat údaje od společností v případech, kdy pro to mají závažný důvod. Pro situace tohoto typu stanoví NOD jasný postup vyřizování žádostí. V souvislosti s ochrannými opatřeními z NOD dále vyplývá ochrana před přístupem státních orgánů třetích zemí, které mohou získat přístup k neosobním údajům, pokud by to bylo v rozporu s právem EU nebo vnitrostátním právem.

Co vše je obsahem NOD?

NOD definuje tři typy subjektů v souvislosti s používáním a sdílením údajů:

1. **Uživatel** – fyzická nebo právnická osoba, která vlastní, pronajímá nebo si půjčuje produkty IoT nebo přijímá související služby[14].[15]
2. **Držitel dat** – fyzická nebo právnická osoba, která má údaje v držení a může k nim poskytnout

přístup.
3. **Příjemce dat** – fyzická nebo právnická osoba, která přijímá údaje od držitele údajů na základě žádosti uživatele.

NOD specifikuje tři typy procesů sdílení údajů tak, aby bylo možné usilovat o vytvoření dodatečné hodnoty z údajů, a to: (1) mezi podniky a spotřebiteli (B2C), (2) mezi podniky a podniky (B2B) a (3) mezi podniky a veřejnou správou (B2G). Aby bylo zajištěno, že procesy sdílení dat mezi jednotlivými stranami budou řádně sladěny a budou fungovat bez problémů, jsou pro každý proces a zúčastněné strany stanoveny určité pokyny a také jednotlivé odpovědnosti a omezení.

Business to consumer (B2C)

NOD má v prvé řadě umožnit uživatelům propojených produktů nebo souvisejících služeb přístup k údajům, které sami vytvářejí při používání těchto produktů a služeb. Mezi propojené produkty mohou patřit například: zařízení pro monitorování zdraví, zařízení pro inteligentní domácnost, ale také například průmyslové stroje, letadla nebo roboti. Propojenou službou, je pak služba, která úzce souvisí s propojeným produktem a umožňuje jeho specifické funkce. Například - koupí-li si uživatel „chytrou“ pračku a nainstaluje si aplikaci, která mu umožní měřit dopad pracího cyklu na životní prostředí na základě údajů z různých čidel uvnitř pračky a podle toho cyklus upravit, bude tato aplikace považována za související službu.[16] NOD se v tomto ohledu zaměřuje právě na strojově generované údaje, které jsou záměrně nebo neúmyslně shromažďovány propojeným produktem (IoT) nebo souvisejícími službami poté, co uživatel provedl určitou akci. Držitel dat je podle NOD povinen poskytnout uživatelům přístup k vygenerovaným údajům.[17]

Business to business (B2B)

NOD dále stanoví pravidla pro situace, kdy má podnik (držitel dat) podle právních předpisů EU nebo vnitrostátních právních předpisů právní povinnost poskytnout údaje jinému podniku (příjemci dat), a to i v souvislosti s údaji IoT. Držitelé dat, kteří jsou povinni údaje sdílet, mohou od příjemce dat požadovat přiměřenou náhradu jako pobídku ke sdílení údajů. Typem údajů, na které se toto nařízení bude vztahovat, jsou údaje v dispozici podniku. Praktickým příkladem tohoto procesu může být situace, kdy uživatelé automobilů poskytnou pojišťovnám přístup k údajům generovaným provozem vozidla. Na základě těchto dat by pojišťovna mohla motivovat k bezpečné jízdě, např. poskytováním slev pojištěncům.

Business to government (B2G)

Třetí z výše zmiňovaných procesů umožňuje orgánům veřejného sektoru přístup k datům, která jsou v držení soukromých subjektů a mohou být pro orgány veřejného sektoru nezbytná k vykonání úkolu ve veřejném zájmu. Přístup k těmto datům je však podmíněn přítomností výjimečné potřeby. Do výjimečné potřeby patří mimořádné veřejné situace[18] a situace, které nejsou mimořádné, ale splňují znak výjimečné potřeby.[19]

NOD si tak klade za úkol zajistit, aby veřejné orgány měly k takovým datům včasný a spolehlivý přístup, aniž by to pro podniky představovalo nepřiměřenou administrativní zátěž.

Vynutitelnost

Aby byla zajištěna aplikace a vymáhání NOD, jsou členské státy EU povinny určit jeden nebo více kompetentních dozorových orgánů. Pokud je určeno více orgánů, musí být jmenován koordinátor dat jako hlavní národní kontaktní bod.

Kromě toho jsou členské státy odpovědné za stanovení sankcí za porušení NOD, přičemž musí zohlednit různé faktory, včetně ročního obratu porušovatele v předchozím finančním roce v EU. Tyto sankce by měly být účinné, přiměřené a odrazující. Podle článku 40 odst. 4 NOD mohou být porušení sdílení osobních údajů předmětem administrativních pokut specifikovaných v GDPR[20] (tj. až do výše 20 milionů EUR nebo čtyř procent z celosvětového ročního obratu, podle toho, která částka je vyšší).[21]

Závěr

DGA a NOD jsou nové nástroje v oblasti správy dat, které stojí na premise toho, že data jsou cenná, představují nevyužité bohatství a měla by být co nejvíce zužitkována. DGA a NOD – zdá se – společně usnadní spolehlivý a bezpečný přístup k datům a podpoří využívaní příslušných dat v klíčových hospodářských odvětvích a oblastech veřejného zájmu. Zároveň lze v souvislosti s těmito předpisy očekávat vytvoření jednotného evropského trhu s daty, což by díky přínosu pro evropskou ekonomiku mělo přinést užitek celé společnosti.

Samuel Kovalčík

Weinhold Legal

Weinhold Legal, s.r.o. advokátní kancelář

Florentinum
Na Florenci 15
110 00 Praha 1

Tel.: +420 225 385 333
Fax: +420 225 385 444
e-mail: wl@weinholdlegal.com

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat).

[2] Tedy podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[3 K dispozici >>> zde.

[4] Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.

[5] Proces, při kterém se osobní údaje upraví tak, aby jednotlivce nebylo možné přímo identifikovat bez dalších informací. Osobní identifikátory se nahradí pseudonymy, což zvyšuje ochranu soukromí, ale data lze v případě potřeby opět propojit s konkrétní osobou, pokud k tomu existuje speciální klíč.

[6] K dispozici >>> zde.

[7] K dispozici >>> zde.

[8] Jednotlivci nebo společnosti, kteří chtějí opakovaně použít stávající údaje, ať už pro výzkum, vývoj produktů, služby nebo jiné účely, při dodržení pravidel ochrany soukromí a bezpečnosti údajů.

[9] Článek 50 NOD.

[10] K dispozici >>> zde.

[11] K dispozici >>> zde.

[12] K dispozici >>> zde.

[13] Článek 2 odst. 5 a odůvodnění 14 NOD.

[14] Digitální služby jiné než služby elektronických komunikací (včetně softwaru), které i) jsou od počátku připojeny k produktu takovým způsobem, že by bez nich připojený produkt nefungoval, nebo ii) jsou následně přidány za účelem zlepšení funkčnosti připojeného produktu.

[15] Článek 2 odst. 6 a odůvodnění17 NOD.

[16] K dispozici >>> zde.

[17] K dispozici >>> zde.

[18] Velké přírodní nebo člověkem způsobené katastrofy, pandemie a kybernetické bezpečnostní incidenty.

[19] Souhrnné anonymizované údaje ze systémů GPS řidičů by mohly být použity k optimalizaci dopravních toků.

[20] Čl. 83 odst. 5 nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (GDPR).

[21] K dispozici >>> zde.

Další články:

- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti