Společné stanovisko Evropského sboru pro ochranu osobních údajů a evropského inspektora ochrany údajů č. 03/2021 k návrhu nařízení Evropského parlamentu a Rady o evropské správě dat (akt o správě dat)

Verze 1.1

Historie verzí

Verze 1.1	9. června 2021	Drobné redakční úpravy
Verze 1.0	10. března 2021	Přijetí společného stanoviska

OBSAH

Evropský sbor pro ochranu osobních údajů a evropský inspektor ochrany údajů

s ohledem na čl. 42 odst. 2 nařízení (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (dále jen „nařízení EUDPR“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI uvedené dohody a protokol 37 k uvedené dohodě, ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018,

PŘIJALI TOTO SPOLEČNÉ STANOVISKO:

1 SOUVISLOSTI

1. Návrh aktu o správě dat (dále jen „návrh“) je schválen v souladu se sdělením o evropské strategii pro data (dále jen „strategie pro data“)[1].

2. Evropský sbor pro ochranu osobních údajů (EDPB) a evropský inspektor ochrany údajů (EIOÚ) berou na vědomí, že podle Komise strategie pro data stanoví, že *„[o]bčané budou daty podloženým inovacím důvěřovat a budou je přijímat pouze tehdy, pokud si budou jisti, že veškeré sdílení osobních údajů v EU bude podmíněno plným dodržováním přísných pravidel EU v oblasti ochrany údajů“*[2].

3. Jak je upřesněno v důvodové zprávě, cílem návrhu *„je podpořit dostupnost dat pro použití, a to zvýšením důvěry ve zprostředkovatele dat a posílením mechanismů pro sdílení dat v celé EU. Nástroj se bude zabývat těmito situacemi:*

   – Zpřístupňování dat veřejného sektoru pro opakované použití v případech, kdy se na tato data vztahují práva jiných osob.

   – Sdílení dat mezi podniky, a to za úplatu v jakékoli podobě.

   – Možnost použít osobní údaje s pomocí „zprostředkovatele sdílení osobních údajů“, který má napomáhat fyzickým osobám při uplatňování jejich práv podle obecného nařízení o ochraně osobních údajů (GDPR).

   – Možnost použít data z altruistických důvodů“[3].

4. Při předkládání návrhu se Komise zejména domnívala, že *„Nové nařízení poskytne rámec pro řádnou správu podporující společné evropské datové prostory a zajistí možnost dobrovolného zpřístupnění dat ze strany jejich držitelů. Doplní připravovaná pravidla pro datové soubory s vysokou hodnotou podle směrnice o otevřených datech, která zajistí bezplatný přístup k určitým datovým souborům v celé EU*

[1] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Evropská strategie pro data, 19. února 2020, COM(2020) 66 final.
[2] Evropská strategie pro data, úvod, strana 1.
[3] Důvodová zpráva, strana 1.

ve strojově čitelném formátu a prostřednictvím standardizovaných rozhraní pro programování aplikací“[4].

5. Strategie pro data též zdůrazňuje, že „*dostupnost dat je zásadní pro trénování systémů v oblasti umělé inteligence, přičemž produkty a služby se rychle přesouvají od rozpoznávání vzorců a tvorby poznání k důmyslnějším prognostickým metodám, a tudíž i k lepšímu rozhodování*“[5].

6. Jak bylo uznáno v důvodové zprávě návrhu, „ *souhra s právními předpisy týkajícími se osobních údajů je obzvláště důležitá. Obecným nařízením o ochraně osobních údajů (GDPR) a směrnicí o soukromí a elektronických komunikacích zavedla EU spolehlivý a důvěryhodný právní rámec pro ochranu osobních údajů a standard pro svět*“[6].

7. EDPB a EIOÚ též upozorňují, že cílem návrhu, na který se odvolává důvodová zpráva, „*je usnadnit sdílení dat, a to mimo jiné posílením důvěry ve zprostředkovatele sdílení dat, jejichž služby se mají podle očekávání využívat v různých datových prostorech. Nemá udělovat, měnit či rušit významná práva týkající se přístupu k údajům a jejich používání. Opatření tohoto druhu se předpokládají u případného aktu o datech (2021)*“[7]. V době práce na tomto společném stanovisku nebyl cíl a obsah takového aktu o datech ještě k dispozici.

2 OBLAST PŮSOBNOSTI SPOLEČNÉHO STANOVISKA

8. Dne 25. listopadu 2020 Komise zveřejnila návrh nařízení Evropského parlamentu a Rady o evropské správě dat (akt o správě dat) (dále jen „návrh“).

9. Dne 25. listopadu 2020 požádala Komise na základě čl. 42 odst. 2 nařízení (EU) 2018/1725 (nařízení EUDPR) o společné stanovisko EDPB a EIOÚ k návrhu.

10. **Návrh je obzvláště důležitý pro ochranu práv a svobod fyzických osob s ohledem na zpracování osobních údajů. Oblast působnosti tohoto stanoviska je omezena na aspekty návrhu týkající se ochrany osobních údajů, které, jak bylo uvedeno, představují klíčový, ne-li nejdůležitější aspekt návrhu.**

11. V této souvislosti EDPB a EIOÚ berou na vědomí, že 3. bod odůvodnění stanoví, že „*[t]ímto nařízením proto není dotčeno nařízení […] (EU) 2016/679*“.

12. EDPB a EIOÚ se domnívají, že základní úkol, kterým je posílit důvěru s cílem usnadnit dostupnost dat a zajistit prospěch pro digitální ekonomiku v EU, je ve skutečnosti založen na **potřebě zajistit a podpořit dodržování a uplatňování *acquis* EU v oblasti ochrany osobních údajů**. Použitelné právo EU v této oblasti, a zejména nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů, GDPR), se považuje za nezbytný předpoklad, z něhož mohou vycházet další legislativní návrhy, aniž by

[4] https://ec.europa.eu/commission/presscorner/detail/cs/QANDA_20_2103
[5] Strategie pro data, strany 2 a 3.
[6] Důvodová zpráva, strana 1.
[7] Důvodová zpráva, strana 1.

ovlivňovaly nebo narušovaly příslušná stávající ustanovení, a to i v případech, kdy jde o pravomoc dozorových úřadů a další aspekty správy[8].

13. Podle EDPB a EIOÚ je tudíž důležité, **aby se v právním textu jednoznačně zamezilo jakémukoli nesouladu a případnému konfliktu s GDPR**. To je nezbytné nejen v zájmu právní jistoty, ale také aby se zamezilo tomu, že návrh přímo či nepřímo ohrozí základní právo na ochranu osobních údajů, stanovené v článku 16 Smlouvy o fungování Evropské unie (SFEU) a v článku 8 Listiny základních práv Evropské unie.

14. EDPB a EIOÚ ve svém společném stanovisku poukazují zejména na nesoulad s právními předpisy EU o ochraně údajů (jakož i s jinými právními předpisy EU, jako je směrnice o otevřených datech) a na problémy, které se týkají například právní jistoty a které by vyplynuly ze vstupu současného návrhu v platnost.

15. Jelikož návrh vyvolává značné množství závažných, často provázaných obav souvisejících s ochranou základního práva na ochranu osobních údajů, jak je podrobně uvedeno v tomto společném stanovisku, **není cílem tohoto společného stanoviska stanovit vyčerpávající seznam problémů, jimiž by se normotvůrci měli zabývat, ani vždy poskytnout alternativní návrhy či navrhnout znění textu**. **Toto společné stanovisko se** místo toho **zaměřuje na hlavní kritické body návrhu**. Zároveň jsou EDPB a EIOÚ i nadále připraveni poskytnout další vyjasnění a vyměňovat si informace s Komisí.

16. EDPB a EIOÚ si jsou též vědomi toho, že legislativní proces týkající se návrhu stále probíhá, a zdůrazňují, že **jsou spolunormotvůrcům připraveni během tohoto procesu poskytovat další rady a doporučení**, a zajistit tak zejména: právní jistotu fyzických osob, hospodářských subjektů a orgánů veřejné moci, řádnou ochranu osobních údajů subjektů údajů v souladu se SFEU, Listinou základních práv EU a *acquis* v oblasti ochrany osobních údajů, udržitelné digitální prostředí včetně nezbytných „kontrol a protivah“.

17. Tato výzva k zapojení úřadů pro ochranu údajů souvisí vzhledem k možným důležitým vazbám na návrh[9] i s jakýmkoli nadcházejícím návrhem evropského aktu o datech.

3 POSOUZENÍ

[8] Viz stanovisko EIOÚ 3/2020 k Evropské strategii pro data, bod 64: „A konečně, EIOÚ zdůrazňuje, že v souvislosti s budoucími mechanismy správy musí být náležitě dodržovány pravomoci **nezávislých dozorových úřadů pro ochranu údajů**. Provádění strategie, které by vedlo k širšímu využívání dat, si navíc vyžádá **výrazné zvýšení zdrojů úřadů pro ochranu údajů** a dalších veřejných orgánů dohledu, zejména z hlediska **technických odborných znalostí a schopností**. Měla by být podporována i spolupráce a společná vyšetřování všech příslušných veřejných orgánů dohledu, včetně dozorových úřadů pro ochranu údajů.“

[9] Posouzení dopadů doprovázející návrh, SWD(2020) 295 final, na straně 6 upřesňuje, že (zvýraznění doplněno): „Současná iniciativa je **prvním krokem dvoufázového přístupu**, který byl oznámen v Evropské strategii pro data. **Iniciativa** bude řešit naléhavou potřebu usnadnit sdílení dat prostřednictvím podpůrného **správního rámce**. **Ve druhém kroku** se Komise bude zabývat otázkami, **kdo kontroluje nebo „vlastní“ údaje, tj. majetkovými právy týkajícími se toho, kdo má přístup k jakým údajům, jaká data může kdo využívat a za jakých okolností**. **Zavedení takových práv** bude zkoumáno v kontextu **aktu o datech (2021)**. V důsledku rozcházejících se zájmů zúčastněných stran a odlišných názorů na to, co je v tomto ohledu rozumné, se tyto otázky stávají předmětem intenzivní debaty, která vyžaduje více času.“

3.1 Obecné poznámky

18. EDPB a EIOÚ uznávají oprávněný cíl, kterým je podporovat dostupnost dat k použití zvýšením důvěry ve zprostředkovatele dat a posílením mechanismů pro sdílení dat v celé EU, a současně zdůrazňují, že ochrana osobních údajů je základním a nedílným prvkem důvěry, kterou by fyzické osoby a organizace měly mít v rozvoj digitální ekonomiky. Návrh nařízení o evropské správě dat (akt o správě dat) je třeba posuzovat také s ohledem na zvýšenou závislost digitální ekonomiky na zpracování osobních údajů a s ohledem na vývoj nových technologií, jako je analytika velkých datových souborů a umělá inteligence.

19. EDPB a EIOÚ zdůrazňují, že zatímco GDPR vychází z nutnosti posílit základní právo na ochranu údajů, návrh se jasně soustřeďuje na uvolnění ekonomického potenciálu opakovaného použití a sdílení dat. Cílem návrhu je tudíž „zlepšit podmínky pro sdílení dat na vnitřním trhu“, jak je uvedeno ve 3. bodě odůvodnění. **EDPB a EIOÚ však konstatují, že návrh, rovněž s přihlédnutím k posouzení dopadů, které je k němu připojeno, řádně nezohledňuje potřebu zajistit a zaručit úroveň ochrany osobních údajů poskytovanou právem EU. EDPB a EIOÚ se domnívají, že tento politický trend směřující k rámci ekonomiky založené na datech bez dostatečného zohlednění aspektů ochrany osobních údajů vzbuzuje vážné obavy, pokud jde o základní práva.** V této souvislosti EDPB a EIOÚ zdůrazňují, že jakýkoli návrh, včetně nadcházejících iniciativ týkajících se dat, jako je evropský akt o datech, který může mít dopad na zpracování osobních údajů, musí zajistit a podporovat dodržování a uplatňování *acquis* EU v oblasti ochrany osobních údajů.

20. **EDPB a EIOÚ dále zdůrazňují, že se model Evropské unie opírá o začleňování jejích hodnot a základních práv v rámci vývoje všech jejích politik a že GDPR musí být považováno za základ, na kterém má být vybudován evropský model správy dat. Jak již bylo uvedeno v různých politických souvislostech, např. při boji proti pandemii COVID-19, právní rámec EU v oblasti ochrany osobních údajů je považován spíše za předpoklad než za překážku rozvoje ekonomiky založené na datech odpovídající unijním hodnotám a zásadám.**

21. EDPB a EIOÚ věří, že toto společné stanovisko poskytne spolunormotvůrcům informace, aby zajistili přijetí legislativního nástroje, který je plně v souladu s *acquis* EU v oblasti ochrany osobních údajů, a zvyšuje tak důvěru udržováním úrovně ochrany poskytované právem EU pod dohledem nezávislých úřadů pro ochranu údajů zřízených podle čl. 16 odst. 2 SFEU.

3.2 Obecné problémy týkající se vztahu návrhu a práva Unie v oblasti ochrany osobních údajů

22. Návrh obsahuje několik odkazů na dodržování GDPR, které stanovuje pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem osobních údajů (viz mimo jiné 3. bod odůvodnění, 28. bod odůvodnění návrhu: „*Jsou-li poskytovatelé služeb sdílení dat správci nebo zpracovateli ve smyslu nařízení (EU) 2016/679, jsou vázáni pravidly stanovenými ve zmíněném nařízení.*“).

23. EDPB a EIOÚ se domnívají, že s ohledem na rozsah zpracování osobních údajů, na který návrh odkazuje, by měl 3. bod odůvodnění obsahovat rovněž odkaz na směrnici (ES) 2002/58 („směrnice o soukromí a elektronických komunikacích“), jelikož je rovněž součástí *acquis* EU v oblasti ochrany osobních údajů, s nímž má být návrh v souladu.

24. Obecněji se EDPB a EIOÚ domnívají, že **duch i litera návrhu nesmí zeslabit úroveň ochrany a musí zajistit plný soulad se všemi zásadami a pravidly** stanovenými v GDPR, aby bylo možné účinně zaručit základní práva na ochranu osobních údajů podle článku 8 Listiny a článku 16 SFEU.

25. Jak je uvedeno v následujících odstavcích tohoto společného stanoviska, EDPB a EIOÚ se s ohledem na výše uvedené domnívají, že **návrh povede k závažným nesrovnalostem s GDPR,** jakož i s dalšími právními předpisy Unie[10], zejména pokud jde o těchto pět aspektů:

a) předmět a oblast působnosti návrhu;

b) definice/terminologie používané v návrhu;

c) právní základ zpracování osobních údajů;

d) stírání rozdílu (při zpracování) mezi osobními a neosobními údaji (a nejasný vztah návrhu a nařízení o volných tocích neosobních údajů);

e) správa/úkoly a pravomoci příslušných subjektů a orgánů, které mají být určeny v souladu s návrhem, s ohledem na úkoly a pravomoci úřadů pro ochranu údajů odpovědných za ochranu základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů, jakož i za usnadňování volného toku osobních údajů v Unii.

A. Předmět a oblast působnosti

26. Podle čl. 1 odst. 2 návrhu: *„Tímto nařízením nejsou dotčena zvláštní ustanovení v jiných právních aktech Unie týkající se přístupu k určitým kategoriím dat či jejich opakovaného použití nebo požadavky související se zpracováváním osobních či neosobních údajů.*

Pokud odvětvový právní akt Unie vyžaduje, aby subjekty veřejného sektoru, poskytovatelé služeb sdílení dat nebo registrované subjekty poskytující služby datového altruismu splňovaly určité

[10] Ačkoli se tato připomínka netýká výhradně zpracování osobních údajů, EDPB a EIOÚ si rovněž všímají případné zmatečnosti a nejasností ohledně toho, jak se návrh bude uplatňovat společně s **nařízením (EU) 2018/1807 o rámci pro volný tok neosobních údajů v Evropské unii**. V této souvislosti je třeba zdůraznit, že definice pojmů „zpracování“, „uživatel“, „profesionální uživatel“ a „požadavek na lokalizaci údajů“, jakož i další ustanovení nařízení o neosobních údajích (viz například článek 6, *Přenesení údajů*), nemusí být **v souladu** s definicemi a ostatními ustanoveními návrhu nebo se s nimi mohou překrývat. Pokud jde o opakované použití dat v držení subjektů veřejného sektoru, která jsou chráněna z důvodů statistické důvěrnosti, je třeba zdůraznit, že navzdory zásadě stanovené v čl. 3 odst. 3 návrhu nejsou podmínky pro opakované použití definované v čl. 5 odst. 3 a 4 v souladu s odvětvovými pravidly stanovenými na úrovni EU pro ochranu důvěrných údajů používaných ke statistickým účelům (viz nařízení Evropského parlamentu a Rady (ES) č. 223/2009 ze dne 11. března 2009 o evropské statistice a zrušení nařízení (ES, Euratom), č. 1101/2008 o předávání údajů, na které se vztahuje statistická důvěrnost, Statistickému úřadu Evropských společenství, nařízení Rady (ES) č. 322/97 o statistice Společenství, rozhodnutí Rady 89/382/EHS, Euratom, kterým se zřizuje Výbor pro statistické programy Evropských společenství, a nařízení Komise (EU) č. 557/2013 ze dne 17. června 2013, kterým se provádí nařízení Evropského parlamentu a Rady (ES) č. 223/2009 o evropské statistice, pokud jde o přístup k důvěrným údajům pro vědecké účely, a kterým se zrušuje nařízení (ES) č. 831/2002).

dodatečné technické, administrativní či organizační požadavky, a to i prostřednictvím režimu udělování oprávnění či certifikace, platí i tato ustanovení zmíněného odvětvového právního aktu Unie."

27. **V zájmu jasnosti doporučují EDPB a EIOÚ do článku 1 návrhu vložit ustanovení jasně a jednoznačně uvádějící, že návrh zachovává nedotčenou úroveň ochrany fyzických osob v souvislosti se zpracováním osobních údajů podle práva Unie a členských států a nijak ji neovlivňuje a že nemění žádné povinnosti a žádná práva stanovená v právních předpisech o ochraně údajů. Toto doplnění by zajistilo větší právní jistotu a zaručuje, že nebude narušeno základní právo na ochranu osobních údajů.**

28. V této souvislosti není jasné, proč je podobné upřesnění obsaženo v čl. 9 odst. 2 návrhu, který zmiňuje poskytovatele služeb sdílení dat[11], a nikoli (obdobně také ve vztahu k subjektům veřejného sektoru, dalším uživatelům, organizacím pro datový altruismus) jako horizontální ustanovení v rámci článku 1 návrhu.

B. Definice návrhu nejsou v souladu s definicemi a klíčovými pojmy nařízení GDPR, a proto je nutné je upravit nebo upřesnit.

29. Definice pojmu „*držitel dat*" podle čl. 2 odst. 5 návrhu: „*právnická osoba nebo subjekt údajů mající v souladu s platnými unijními nebo vnitrostátními právními předpisy právo umožnit přístup k určitým osobním nebo neosobním údajům nebo sdílet takové údaje, nad nimiž má kontrolu*" není v souladu se zastřešujícími zásadami GDPR ani s jeho literou.

30. V této souvislosti EDPB a EIOÚ poznamenávají, že právní nejistota může vyplynout ze skutečnosti, že GDPR nezmiňuje právo subjektu údajů poskytnout přístup ke svým osobním údajům nebo je sdílet s třetími stranami, natož pak rovnocenné právo pro právnickou osobu, které lze vyvodit z uvedené definice „držitele dat". GDPR spíše každé fyzické osobě zaručuje právo na ochranu osobních údajů, které se jí týkají, což odkazuje na komplexní soubor pravidel pro zpracování osobních údajů, která jsou závazná pro každý subjekt zpracovávající údaje (správce / společný správce údajů) nebo subjekt zpracovávající údaje jménem správce údajů (zpracovatel)[12].

---

[11] Ustanovení čl. 9 odst. 2 uvádí: „*Touto kapitolou není dotčeno uplatňování jiných unijních a vnitrostátních právních předpisů na poskytovatele služeb sdílení dat, včetně pravomoci dozorových úřadů zajistit dodržování platných právních předpisů, zejména právních předpisů o ochraně osobních údajů a právních předpisů v oblasti hospodářské soutěže*."

[12] Viz též 6. a 7. bod odůvodnění GDPR (zvýraznění doplněno):
„(6) Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Fyzické osoby stále častěji své osobní údaje zveřejňují, a to i v globálním měřítku. Technologie změnily ekonomiku i společenský život a měly by dále usnadňovat volný pohyb osobních údajů v rámci Unie a předávání do třetích zemí a mezinárodním organizacím a zároveň zajistit **vysokou úroveň ochrany osobních údajů**.
(7) Tento vývoj vyžaduje **pevný a soudržnější rámec pro ochranu osobních údajů** v Unii, jenž by se opíral o **důsledné vymáhání práva**, a to s ohledem na nezbytnost nastolit **důvěru**, která umožní rozvoj digitální ekonomiky na celém vnitřním trhu. **Fyzické osoby by měly mít možnost kontrolovat své vlastní osobní údaje**. Měla by být posílena **právní a praktická jistota** fyzických osob, hospodářských subjektů a orgánů veřejné moci."

31. **V této souvislosti se EIOÚ a EDPB domnívají, že spíše než konstatování, že právnická osoba má právo udělit přístup k osobním údajům nebo je sdílet, by bylo vhodnější uvést, zda a za jakých podmínek může být určité zpracování osobních údajů provedeno, či nikoli.**

32. EDPB a EIOÚ by chtěli konkrétně upřesnit, že přístup k osobním údajům i jejich sdílení představují zpracování osobních údajů podle čl. 4 odst. 2 GDPR.

33. Podle právních předpisů o ochraně údajů je zpracování osobních údajů zákonné, pokud subjekt údajů (identifikovaná nebo identifikovatelná fyzická osoba, jíž se osobní údaje týkají) dal souhlas se zpracováním svých osobních údajů pro jeden nebo více konkrétních účelů nebo pokud lze oprávněně použít jiný vhodný právní základ podle článku 6 GDPR.

34. Výše uvedené úvahy jsou učiněny zejména s ohledem na článek 8 Listiny: „*1. Každý má právo na ochranu osobních údajů, které se ho týkají. 2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem*.“

35. EDPB a EIOÚ znepokojuje též znění 14. bodu odůvodnění návrhu (podtržení doplněno): „*Společnosti a subjekty údajů by měly být schopny důvěřovat tomu, že se opakované použití určitých kategorií chráněných dat, která jsou v držení veřejného sektoru, uskuteční způsobem, jenž respektuje jejich práva a zájmy*.“; čl. 11 odst. 6 uvádějící „*záruky, jež držitelům dat a uživatelům dat umožňují získat přístup k údajům v případě platební neschopnosti*“; jakož i znění článku 19 „*Zvláštní požadavky na ochranu práv a zájmů subjektů údajů a právních subjektů s ohledem na jejich údaje*“, kde se v čl. 19 odst. 1 písm. a) uvádí: „*o cílech obecného zájmu, pro něž povoluje zpracovávání jejich údajů [údajů držitelů dat] uživatelem dat, a to snadno srozumitelným způsobem“.*

36. V této souvislosti EDPB a EIOÚ poznamenávají, že práva a zájmy subjektu údajů s ohledem na jeho osobní údaje na jedné straně a práva a zájmy právnických osob s ohledem na informace, které se jich týkají, na straně druhé nejsou stejného druhu (práva a zájmy právnických osob se netýkají lidské důstojnosti ani práva na soukromí a ochranu údajů, ale spíše práv průmyslového vlastnictví, jako jsou obchodní tajemství, patenty a ochranné známky). Proto by vzhledem k výše uvedené heterogenitě byla zmíněná ustanovení nejen pojmově „nesourodá“, ale také obtížně proveditelná a jako taková by prohlubovala právní nejistotu. Například u platební neschopnosti (uvedené v čl. 11 odst. 6) by se zavedené záruky umožňující držitelům dat získat přístup k neosobním údajům v praxi podstatně lišily od podmínek a omezení dalšího zpracování osobních údajů. Jedná se skutečně o rozdílné problémy, které vyžadují odlišná řešení[13], a odkaz na oba tyto problémy v rámci povinnosti poskytovatele služeb sdílení dat zajistit kontinuitu poskytování služeb (včetně sdílení osobních údajů) je přinejmenším matoucí, ne-li zjevně v rozporu s GDPR.

[13] Například u platební neschopnosti je třeba věnovat pozornost skutečnosti, že v jejím důsledku dojde ke změně správy zpracování údajů. Nový správce zejména stanoví, jaké údaje lze zpracovat; určí účely, pro které byly údaje původně získány; stanoví zákonný základ pro sdílení údajů; zajistí soulad se zásadami ochrany údajů, zejména zákonnost, spravedlnost a transparentnost; informuje subjekty údajů o změnách týkajících se zpracování jejich údajů a bere v úvahu, že subjekty údajů mohou uplatnit své právo vznést námitku.

37. Novou definicí zavedenou návrhem je též definice „uživatele dat“[14] podle čl. 2 odst. 6, jejíž vzájemný vztah – v případě osobních údajů – s definicí příjemce[15] podle čl. 4 odst. 9 GDPR je nejasný. V této souvislosti bereme na vědomí, že čl. 11 odst. 1 návrhu stanoví: „Poskytovatel nesmí použít data, pro něž poskytuje služby, k jiným účelům, než je možnost uživatelů dat nakládat s nimi […].“ Toto ustanovení, chápané ve spojení s definicí „uživatele dat“, vede k právní nejistotě z důvodu rozdílných pojmů *„příjemce“* podle GDPR a *„uživatele dat“* podle návrhu, což by vedlo k problémům s uplatňováním v praxi. Definice podle čl. 2 odst. 6 by navíc mohla být zavádějící, pokud by se chápala jako odkaz na fyzickou nebo právnickou osobu, která je oprávněna (má právo?) používat osobní údaje pro komerční a nekomerční účely. Odkaz na takové „oprávnění“ a význam (jeho právní zdroj a účinek) takového „oprávnění“ je též nejasný.

38. Nejasný je navíc také vzájemný vztah mezi pojmem uživatel dat jako „fyzickou nebo právnickou osobou [oprávněnou použít údaje pro komerční a nekomerční účely]“ a pojmy správce, společný správce nebo zpracovatel podle GDPR. Návrh dále odkazuje na případnou kvalifikaci správce nebo zpracovatele a jejich povinnosti podle GDPR pro poskytovatele služeb sdílení dat[16], nikoli však pro uživatele dat nebo pro organizace pro datový altruismus (navzdory skutečnosti, že i ti mohou být správcem, společným správcem nebo zpracovatelem podle GDPR).

39. **Obecněji EDPB a EIOÚ zdůrazňují, že návrh by měl definovat role každého typu „aktéra“ (poskytovatel služeb sdílení dat, organizace pro datový altruismus, uživatel dat) se zřetelem na právní předpisy o ochraně osobních údajů (správce údajů, zpracovatel nebo společný správce) nejen proto, aby se předešlo nejednoznačnosti ohledně příslušných povinností podle GDPR, ale také aby se zvýšila srozumitelnost právního textu.**

40. Podobné problémy, konkrétně **nejasný vztah k definicím a pravidlům stanoveným v GDPR**, se týkají definice „sdílení dat“ podle čl. 2 odst. 7 návrhu (mimo jiné uvádějící „společné či individuální použití sdílených dat“). Pokud jde o osobní údaje, je přinejmenším matoucí také společné používání osobních údajů (držitelem dat, právnickou osobou i uživatelem dat), a to buď přímo, nebo prostřednictvím zprostředkovatele.

41. Podobné obavy, jak je podrobněji uvedeno níže, se týkají pojmu „svolení [právních subjektů s opakovaným použitím dat]“, který však v návrhu není definován.

42. Z hlediska ochrany osobních údajů je problematická i definice „metadat“ v čl. 2 odst. 4, jelikož odkazuje na „shromážděná data o jakékoli činnosti fyzické nebo právnické osoby za účelem poskytování služby sdílení dat, včetně údajů o datu a čase a geolokačních údajů, doby trvání činnosti, kontaktů s jinými fyzickými či právnickými osobami, které navázala osoba využívající službu“. Taková data mohou zahrnovat osobní údaje.

---

[14] Ustanovení čl. 2 odst. 6 návrhu: „‚**uživatelem dat**‘ [se rozumí] **fyzická nebo právnická osoba**, která má zákonný přístup k **určitým** osobním nebo neosobním údajům a je **oprávněna použít tyto údaje** pro komerční či nekomerční účely“.

[15] Podle definice stanovené v GDPR, v čl. 4 odst. 9, „[se] ‚příjemcem‘ [rozumí] fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli […]“.

[16] Viz 28. bod odůvodnění: „Jsou-li poskytovatelé služeb sdílení dat správci nebo zpracovateli ve smyslu nařízení (EU) 2016/679, jsou vázáni pravidly stanovenými ve zmíněném nařízení.“

43. Jak je podrobněji uvedeno v tomto společném stanovisku, s ohledem na čl. 11 odst. 2 lze návrh vykládat v tom smyslu, že vytváří právní základ pro zpracování metadat. Článek 11 návrhu patrně jako podmínku pro poskytování služby sdílení dat stanoví, že by poskytovatel měl být skutečně schopen použít výše uvedená metadata „k rozvoji takovéto služby [sdílení dat]“. V právním textu se mimo jiné neuvádí potřeba, aby se poskytovatel služeb sdílení dat opíral o odpovídající právní základ pro zpracování osobních údajů podle čl. 6 odst. 1 GDPR.

44. **Obecněji řečeno, jelikož není návrhem dotčeno GDPR, jak je výslovně uvedeno v samotném návrhu, měly by se podle EDPB a EIOÚ použít definice, které předpokládá nařízení GDPR a které by neměly být návrhem implicitně pozměněny ani odstraněny, a nové definice, pokud se týkají zpracování osobních údajů, by neměly „ve skutečnosti“ obsahovat „pravidla“, která jsou v rozporu s duchem a literou GDPR.**

45. Toto upřesnění je zvláště důležité z důvodu kumulativního účinku, pokud jde o nejasnosti a právní nejistotu vyplývající z návrhu, kdy stejné ustanovení obsahuje více než jednu nejasnou definici (viz například čl. 7 odst. 2 písm. c) návrhu uvádějící „získávání souhlasu *nebo* svolení k opakovanému použití pro altruistické a jiné účely ze strany dalších uživatelů, a to v souladu se zvláštními rozhodnutími držitelů dat“).

46. **Vzhledem k výše uvedenému EDPB a EIOÚ doporučují návrh vyjasnit a upravit, aby bylo zajištěno, že – pokud jde o osobní údaje – nezůstane v rozporu s definicemi a pojmy GDPR.**

C. Aby se předešlo vzniku právní nejistoty, měl by návrh upřesnit použitelný právní základ v GDPR pro zpracování osobních údajů.

47. EDPB a EIOÚ konstatují, že návrh v několika ustanoveních zmiňuje „svolení držitelů dat“ s použitím dat:

– v čl. 5 odst. 6: „*podpoří subjekt veřejného sektoru další uživatele žádající o souhlas subjektů údajů a/nebo svolení právních subjektů, jejichž práva a zájmy mohou být tímto opakovaným použitím dotčeny, je-li to proveditelné bez nepřiměřených nákladů pro veřejný sektor“, což je upřesněno v 11. bodě odůvodnění: „Subjekty veřejného sektoru by měly případně usnadnit opakované použití dat na základě souhlasu subjektů údajů či svolení právnických osob, pokud jde o opakované použití dat, která se jich týkají, a to prostřednictvím náležitých technických prostředků.“,*

– v čl. 7 odst. 2 písm. c): *„případně napomáhání subjektům veřejného sektoru při získávání souhlasu nebo svolení k opakovanému použití pro altruistické a jiné účely ze strany dalších uživatelů, a to v souladu se zvláštními rozhodnutími držitelů dat, […]“,*

– v čl. 11 odst. 11: *„pokud poskytovatel poskytuje nástroje k získání souhlasu od subjektů údajů nebo svolení ke zpracování dat zpřístupněných právnickými osobami, upřesní jurisdikci nebo jurisdikce, v nichž mají být data použita“,*

– v čl. 19 odst. 3: „*Pokud subjekt zapsaný v rejstříku uznaných organizací pro datový altruismus poskytuje nástroje k získání souhlasu od subjektů údajů nebo svolení ke zpracování údajů zpřístupněných právnickými osobami, upřesní jurisdikci nebo jurisdikce, v nichž se mají data používat“, což je upřesněno v 36. bodě odůvodnění: „Právnické osoby by mohly udělit svolení ke zpracovávání svých neosobních údajů pro celou řadu účelů, jež nejsou v době udělení svolení vymezeny.*“

48. EDPB a EIOÚ v této souvislosti konstatují, že ve většině případů není jasné, zda by předmětem svolení bylo opakované použití osobních nebo neosobních údajů, nebo obou těchto druhů údajů.

49. EDPB a EIOÚ rovněž poznamenávají, že v případě zpracování osobních údajů nemůže **„svolení" uvedené v návrhu nahradit nutnost jednoho vhodného právního důvodu podle čl. 6 odst. 1 GDPR pro zákonné zpracování osobních údajů**. Jinými slovy, podle GDPR je zpracování zákonné, pouze pokud se uplatňuje nejméně jeden z právních základů podle čl. 6 odst. 1 nařízení GDPR a pouze v odpovídajícím rozsahu. Návrh by měl tento aspekt jasně upřesnit, aby se předešlo nejednoznačnosti.

50. Ve skutečnosti dokonce i výklad pojmu „svolení" (který však má být definován v právním textu návrhu) jako „rozhodnutí (obchodní volba) právnické osoby povolit zpracování osobních údajů, pokud má tato právnická osoba právní základ podle čl. 6 odst. 1 GDPR povolující takové zpracování", je třeba poznamenat, že se zdá, že doslovný výklad některých ustanovení návrhu nepodporuje tento výklad v souladu s GDPR, jelikož například uvádějí: *„Pokud opakované použití dat nelze umožnit v souladu s povinnostmi stanovenými v odstavcích 3 až 5 a neexistuje žádný jiný právní základ pro předání dat podle nařízení (EU) 2016/679, podpoří subjekt veřejného sektoru další uživatele žádající o souhlas subjektů údajů a/nebo svolení právních subjektů"* (čl. 5 odst. 6 návrhu)[17]. V těchto případech se „svolení" jeví jako alternativa přinejmenším jednoho právního základu (souhlasu subjektu údajů) stanoveného v článku 6 GDPR.

51. Šestý bod odůvodnění návrhu je též nejasný, pokud jde o vhodný právní základ pro zpracování osobních údajů, jelikož zmiňuje povinnost „obecně" se opírat o právní základ pro zpracování osobních údajů stanovený v článku 6 GDPR[18].

52. Z jiného hlediska, jak je podrobněji uvedeno v tomto stanovisku, EDPB a EIOÚ poukazují na potřebu **vyjasnit vztah mezi různými scénáři předpokládanými v návrhu a v čl. 6 odst. 4 GDPR**, což by upravovalo situace, kdy zpracování osobních údajů pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů.

53. **V tomto smyslu se s ohledem na cíl a obsah návrhu EDPB a EIOÚ domnívají, že návrh nelze uplatňovat jako právo Unie, které v demokratické společnosti představuje nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1 GDPR, aby bylo odůvodněno zpracování pro jiný účel, než pro který byly osobní údaje původně shromážděny, pokud takové zpracování není založeno na souhlasu v souladu s čl. 6 odst. 4 GDPR.**

54. **Vzhledem k výše uvedenému doporučují EDPB a EIOÚ v právním textu návrhu upřesnit, že pokud jde o osobní údaje, musí se jejich zpracování vždy opírat o vhodný právní základ podle článku 6 GDPR.**

55. Jako příklad možné nesrovnalosti týkající se právního základu zpracování osobních údajů můžeme uvést ustanovení čl. 11 odst. 2 návrhu, podle kterého *„metadata získaná při poskytování služby sdílení dat lze použít pouze k rozvoji takovéto služby"*. V této souvislosti připomínáme, že metadata uvedená

[17] Viz rovněž čl. 7 odst. 2 písm. c), čl. 11 odst. 11, čl. 19 odst. 3 návrhu uvedené výše.
[18] Šestý bod odůvodnění návrhu zejména uvádí (zvýraznění doplněno): „Co se týká **obecně** osobních údajů, zpracovávání osobních údajů by mělo být založeno na jednom či více důvodech zpracování stanovených v článku 6 nařízení (EU) 2016/679."

v návrhu[19] mohou představovat informace týkající se identifikované nebo identifikovatelné fyzické osoby a v tomto případě musí být zpracována v souladu s pravidly ochrany údajů a zejména s pravidly týkajícími se právního základu zpracování. Jak je však uvedeno v bodě 51 tohoto stanoviska, tímto základním aspektem se návrh nezabývá.

56. **V této věci se EDPB a EIOÚ obecněji domnívají, že výše uvedené ustanovení, stejně jako jakékoli jiné ustanovení návrhu, neposkytuje samostatný právní základ pro opakované použití osobních údajů uživateli dat a pro činnosti zpracování vykonávané poskytovateli služeb sdílení dat nebo organizacemi pro datový altruismus, a to z důvodu, že nesplňuje kritéria podle čl. 6 odst. 3 pro zpracování uvedená v čl. 6 odst. 1 písm. c) a e)[20] GDPR.**

D. Stírání rozdílu mezi osobními a neosobními údaji (mezi jejich zpracováním) a nejasný vztah návrhu k nařízení o volných tocích neosobních údajů

57. Obecně se EDPB a EIOÚ domnívají, že hlavním kritickým bodem návrhu s ohledem na ochranu osobních údajů je – možná z důvodu výše uvedených případů neslučitelnosti nebo přinejmenším nejednoznačnosti právního textu – stírání rozdílu mezi zpracováním neosobních údajů, upraveným v některých aspektech podle nařízení (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný pohyb neosobních údajů v Evropské unii (dále jen „nařízení o volném toku neosobních údajů“) [21], a zpracováním osobních údajů, které je upraveno v *acquis* týkajícím se ochrany údajů a vychází z jiných zásad.

58. V této souvislosti EDPB a EIOÚ zdůrazňují, že se rozdíl mezi kategoriemi osobních a neosobních údajů uplatňuje v praxi obtížně. V praxi lze ve skutečnosti z kombinace neosobních údajů odvodit nebo vytvořit osobní údaje, tj. údaje vztahující se k identifikované nebo identifikovatelné osobě[22], zejména pokud jsou neosobní údaje výsledkem anonymizace osobních údajů, a jde tak o informace původně se týkající fyzických osob. Kromě toho ve scénářích předpokládaných v návrhu v oblasti zvýšení dostupnosti, opakovaného použití a sdílení informací, které by „umožňovaly detekci souvislostí na základě „dat velkého objemu“ nebo strojové učení“[23], platí, že čím více neosobních údajů se kombinuje

---

[19] Podle čl. 2 odst. 4 návrhu se „‚metadaty‘ [rozumí] shromážděná data o jakékoli činnosti fyzické nebo právnické osoby za účelem poskytování služby sdílení dat, včetně údajů o datu a čase a geolokačních údajů, doby trvání činnosti, kontaktů s jinými fyzickými či právnickými osobami, které navázala osoba využívající službu“.

[20] „3. Základ pro zpracování podle odst. 1 písm. c) a e) musí být stanoven:
a) právem Unie nebo b) právem členského státu, které se na správce vztahuje.
Účel zpracování musí vycházet z tohoto právního základu, nebo pokud jde o zpracování uvedené v odst. 1 písm. e), musí být toto zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce. Tento právní základ může obsahovat konkrétní ustanovení pro přizpůsobení uplatňování pravidel tohoto nařízení, včetně obecných podmínek, kterými se řídí zákonnost zpracování správcem, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupů zpracování, jakož i dalších opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace, při nichž dochází ke zpracování, než stanoví kapitola IX. Právo Unie nebo členského státu musí splňovat cíl veřejného zájmu a musí být přiměřené sledovanému legitimnímu cíli.“

[21] Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii (Text s významem pro EHP), Úř. věst. L 303, 28.11.2018, s. 59.

[22] Viz stanovisko EIOÚ č. 3/2020 k Evropské strategii pro data, bod 30.

[23] Důvodová zpráva, strana 3.

s jinými dostupnými informacemi, tím obtížnější bude zajistit anonymizaci z důvodu zvýšeného rizika opětovné identifikace pro subjekty údajů. S ohledem na tento scénář by proto měla být v každém případě zajištěna základní práva subjektů údajů na soukromí a ochranu údajů v různých kontextech předpokládaných návrhem.

59. Zároveň mohou nastat případy neosobních údajů, na které se GDPR nevztahuje a které se od svého vzniku netýkají fyzických osob. Jedná se například o neosobní údaje ze snímačů vibrací v průmyslových strojních zařízeních kombinované s jinými neosobními údaji, např. s geolokací strojního zařízení. Takovéto neosobní údaje nepotřebují stejnou úroveň záruk jako neosobní údaje, které jsou výsledkem anonymizace osobních údajů, protože pouze ty (podobně pseudonymizované údaje) jsou pravděpodobně vystaveny riziku opětovné identifikace.

60. **Aby se předešlo nejasnostem ohledně toho, jak by se návrh uplatňoval „společně s GDPR“, doporučují EDPB a EIOÚ přepracovat návrh tak, aby lépe zohledňoval rozdíl mezi osobními a neosobními údaji a také mezi různými typy neosobních údajů.**

61. Bez ohledu na obavy, které již vyjádřil EIOÚ, pokud jde o koncepci smíšeného souboru údajů a „neoddělitelně propojené“ osobní a neosobní údaje[24], EDPB a EIOÚ připomínají, že podle čl. 2 odst. 2 nařízení o volném toku neosobních údajů platí toto: „*V případě souborů údajů obsahujících jak osobní, tak neosobní údaje se toto nařízení vztahuje na část souboru údajů s neosobními údaji. Pokud jsou osobní a neosobní údaje v souboru údajů neoddělitelně propojeny, není tímto nařízením dotčeno použití nařízení (EU) 2016/679*.“ V důsledku toho se na smíšený soubor dat budou zpravidla vztahovat povinnosti správců údajů a zpracovatelů a práva subjektu údajů stanovená GDPR. Tato úvaha je v kontextu návrhu zvláště významná, protože je možné, že ve většině případů by soubory dat sdílené prostřednictvím poskytovatele služeb sdílení dat nebo organizace pro datový altruismus obsahovaly také osobní údaje. Jelikož neexistuje „třetí kategorie“ mezi osobními a neosobními údaji, nezměnilo by to povahu a „právní režim“ souboru dat jako osobních údajů[25].

62. **Vzhledem k výše uvedenému upozorňují EDPB a EIOÚ na riziko, že návrh vytvoří souběžný soubor pravidel, která nejsou v souladu s GDPR ani s nařízením o volném toku neosobních údajů, a tím jej tedy oslabují a způsobují potíže při uplatňování v praxi.**

E. Správa/úkoly a pravomoci příslušných subjektů a orgánů, které mají být určeny v souladu s návrhem, a úkoly a pravomoci úřadů pro ochranu údajů

63. Návrh předpokládá, že členské státy určí příslušné subjekty, jež by podpořily subjekty veřejného sektoru, které poskytují přístup k opakovanému použití dat (kapitola II návrhu), a že budou určeny

[24] Viz Připomínky EIOÚ k návrhu nařízení Evropského parlamentu a Rady o rámci pro volný tok neosobních údajů v Evropské unii vydané dne 8. června 2018 na adrese: https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf.

[25] Viz rovněž sdělení Komise Evropskému parlamentu a Radě, *Pokyny k nařízení o rámci pro volný tok neosobních údajů v Evropské unii*, na adrese: https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union.

příslušné orgány pro sledování souladu s ustanoveními, která se týkají služeb sdílení dat a datového altruismu (kapitoly III a IV návrhu).

64. **EDPB a EIOÚ obecněji zastávají názor, že existuje riziko zásahů příslušných subjektů a orgánů určených podle návrhu do příslušnosti a úkolů nezávislých orgánů pro ochranu údajů, jelikož mnoho úkolů příslušných subjektů a orgánů určených podle návrhu souvisí se zpracováním osobních údajů. Určení jiných příslušných orgánů/subjektů, než jsou úřady pro ochranu údajů, by proto mohlo být skutečnou komplikací pro digitální aktéry a subjekty údajů a také by mohlo ovlivnit soulad z hlediska sledování toho, jak jsou uplatňována ustanovení GDPR. Pokud bude určení příslušných subjektů a orgánů ponecháno na uvážení členských států, může hrozit i nejednotnost a rozdílnost regulačních přístupů v celé Unii.**

3.3 Opakované použití určitých kategorií chráněných dat v držení subjektů veřejného sektoru

3.3.1 Vztah návrhu ke směrnici o otevřených datech a ke GDPR

65. Zatímco důvodová zpráva uvádí, že návrh *„doplňuje směrnici Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru (dále jen „směrnice o otevřených datech“)*[26] *“*, 5. bod odůvodnění blíže upřesňuje, že *„[s]měrnice (EU) 2019/1024 i odvětvové právní předpisy zajišťují, aby veřejný sektor činil snadno přístupnými pro účely jejich použití a opakovaného použití více dat, která vytváří. Určité kategorie dat (důvěrné údaje obchodní povahy, data, na něž se vztahuje statistická důvěrnost, data chráněná právy duševního vlastnictví třetích stran, včetně obchodního tajemství a osobních údajů, jež nejsou dostupné na základě zvláštních vnitrostátních či unijních právních předpisů, jako je nařízení (EU) 2016/679 a směrnice (EU) 2016/680), často nejsou ve veřejných databázích zpřístupněny, a to ani pro výzkumné či inovativní činnosti. Kvůli citlivosti těchto dat musí být před jejich zpřístupněním splněny určité technické a právní procesní požadavky, aby bylo zajištěno dodržení práv, jež k těmto datům mají jiné osoby. Splnění těchto požadavků je obvykle náročné na čas a znalosti. To má za následek nedostatečné využívání těchto dat. Ačkoli některé členské státy zavádějí struktury a procesy a někdy přijímají právní předpisy k usnadnění opakovaného použití tohoto druhu, neplatí to pro celou Unii.“*

66. EDPB a EIOÚ podotýkají, že navzdory výše uvedeným upřesněním se styčná plocha návrhu se „směrnicí o otevřených datech“ nezdá být jasná. Zejména by mohla vzniknout právní nejistota ohledně rozšířeného opakovaného použití informací veřejného sektoru, které by se podle článku 3 (Kategorie údajů) návrhu vztahovalo na:

„[…] data v držení subjektů veřejného sektoru, která jsou chráněna z důvodů:

a) obchodního tajemství;

b) statistické důvěrnosti;

c) ochrany práv duševního vlastnictví třetích stran;

[26] Úř. věst. L 172, 26.6.2019, s. 56.

d) ochrany osobních údajů“.

67. Důvodová zpráva k návrhu [27] neobjasňuje dostatečně rozsah takového rozšířeného opakovaného použití a vzájemný vztah návrhu a směrnice o otevřených datech. Navíc pod stejné „zastřešení“ (jako „*respektování práv jiných osob*“, což není vhodné s ohledem na ochranu osobních údajů) vkládá „*ochran[u] osobních údajů, avšak rovněž ochran[u] práv duševního vlastnictví a obchodního tajemství*“.

68. Lze tvrdit, že formulace „*data v držení subjektů veřejného sektoru, která jsou chráněna z důvodů*“ mimo jiné „*ochrany osobních údajů*“ (čl. 3 písm. d)) je současně:

– politováníhodná, neboť naznačuje myšlenku regulace ochrany údajů, která *brání* volnému pohybu osobních údajů, místo aby stanovovala pravidla jejich volného toku a zároveň chránila práva a zájmy dotčených osob, *a*

– zčásti nepřesná, jelikož směrnice o otevřených datech místo toho, aby osobní údaje ze své oblasti působnosti vylučovala [28], v čl. 1 odst. 2 písm. h) stanoví, že [směrnice o otevřených datech se nevztahuje na] „*dokumenty, k nimž je vyloučen nebo omezen přístup na základě režimů přístupu z důvodu ochrany osobních údajů, a podle těchto režimů přístupné části dokumentů, které obsahují osobní údaje, jejichž opakované použití bylo právně vymezeno jako jednání v rozporu s právními předpisy na ochranu osob v souvislosti se zpracováním osobních údajů nebo jako jednání oslabující ochranu soukromí a osobnosti jednotlivce, zejména v souladu s unijním nebo vnitrostátním právem týkajícím se ochrany osobních údajů*“[29].

69. Poslední aspekt je však upřesněn v 7. bodě odůvodnění návrhu[30]. V této souvislosti se EDPB a EIOÚ pozastavují nad tím, proč tato důležitá záležitost (jakož i mnoho dalších záležitostí týkajících se ochrany osobních údajů) je zahrnuta do bodu odůvodnění, ale ne do věcné části návrhu.

70. Podle čl. 3 odst. 1 směrnice o otevřených datech navíc do oblasti působnosti směrnice spadají a mohou být zpřístupněny pro opakované použití v souladu s podmínkami stanovenými v téže směrnici, jakož i v souladu s požadavky právních předpisů o ochraně údajů osobní údaje, na které se tato výjimka nevztahuje, které jsou volně přístupné podle unijních nebo vnitrostátních režimů přístupu a které jsou opakovaně použitelné pro slučitelná použití, aniž je oslabena ochrana soukromí a osobnosti fyzické

---

[27] Viz strana 7: „*Kapitola II vytváří mechanismus pro* ***opakované použití určitých kategorií chráněných dat veřejného sektoru,*** *které je* ***podmíněno respektováním práv jiných osob*** *(zejména z důvodů ochrany osobních údajů, avšak rovněž ochrany práv duševního vlastnictví a obchodního tajemství). Tímto mechanismem nejsou dotčeny odvětvové předpisy EU týkající se přístupu k těmto datům a jejich opakovaného použití.* ***Opakované použití těchto dat nespadá do oblasti působnosti směrnice (EU) 2019/1024*** *(směrnice o otevřených datech). Ustanovení této kapitoly nezakládají právo na opakované použití těchto dat, nýbrž stanoví soubor harmonizovaných základních podmínek, za nichž může být povoleno opakované použití takovýchto dat (např. požadavek týkající se zákazu výhradních dohod).*“

[28] Viz článek 1 směrnice o otevřených datech.

[29] V této souvislosti viz též 52. a 53. bod odůvodnění, jakož i čl. 1 odst. 4 a článek 10 směrnice o otevřených datech, přičemž článek 10 se zabývá konkrétně údaji z výzkumu.

[30] „*[Údaje], na něž se vztahuje toto nařízení,* ***nespadají do oblasti působnosti směrnice (EU) 2019/1024****, která vylučuje data, jež nejsou dostupná kvůli obchodnímu tajemství a statistické důvěrnosti, a data, k nimž mají práva duševního vlastnictví třetí strany.* ***Osobní údaje nespadají do oblasti působnosti směrnice (EU) 2019/1024, pokud režim přístupu*** *vylučuje či omezuje přístup k takovýmto datům z důvodů ochrany údajů, soukromí a osobnosti jednotlivce, zejména v souladu s pravidly ochrany údajů.*“ (zvýraznění doplněno)

osoby. Ve skutečnosti, jak je uvedeno ve 154. bodě odůvodnění GDPR, právní předpisy EU o opakovaném použití informací veřejného sektoru *„ponechávají nedotčenu a nijak neovlivňují úroveň ochrany fyzických osob v souvislosti se zpracováním osobních údajů podle práva Unie a členských států, a zejména nemění povinnosti a práva podle nařízení [GDPR]“*. V tomto smyslu by normotvůrce EU měl při zavádění nových zásad a pravidel opakovaného použití informací veřejného sektoru stanovit nezbytnou harmonizaci takového opakovaného použití s právem na ochranu osobních údajů podle GDPR[31].

71. **EDPB a EIOÚ tudíž zdůrazňují, že pravidla směrnice o otevřených datech spolu s pravidly nařízení GDPR již stanovují mechanismy umožňující sdílet osobní údaje v držení subjektů veřejného sektoru způsobem, který je v souladu s požadavky upravujícími ochranu základních práv fyzických osob. EDPB a EIOÚ proto doporučují sladit kapitolu II návrhu se stávajícími pravidly o ochraně osobních údajů stanovenými v GDPR a se směrnicí o otevřených datech, aby bylo zajištěno, že úroveň ochrany osobních údajů v EU nebude oslabována, a aby se zároveň zamezilo tomu, že tento nesoulad vytváří právní nejistotu pro fyzické osoby, orgány veřejného sektoru a další uživatele. Aniž jsou dotčeny další údaje o dopadu pravidel návrhu, která upravující opakované použití určitých kategorií chráněných dat v držení subjektů veřejného sektoru, na právo fyzických osob na soukromí a ochranu údajů uvedené v tomto společném stanovisku, mohly by být osobní údaje případně z jeho působnosti vyloučeny.**

3.3.2 Článek 5: podmínky opakovaného použití dat subjekty veřejného sektoru

72. Podmínky opakovaného použití dat v držení subjektů veřejného sektoru jsou stanoveny v článku 5 návrhu, jak je uvedeno v 11. bodě odůvodnění. V této souvislosti se EDPB a EIOÚ domnívají, že návrh vzbuzuje určité obavy.

73. **EDPB a EIOÚ opakují, že veškeré zpracování osobních údajů uvedené v návrhu musí probíhat v naprostém souladu s GDPR, a musí být tedy doprovázeno příslušnými zárukami ochrany údajů. To znamená, že opakované použití osobních údajů by mělo v souladu s článkem 5 GDPR vždy dodržovat zásady zákonnosti, korektnosti a transparentnosti, jakož i účelového omezení, minimalizace údajů, přesnosti, omezení uložení, integrity a důvěrnosti.**

74. V tomto scénáři jsou korektnost, transparentnost a účelové omezení zásadními zárukami, které mají vzbudit důvěru mezi fyzickými osobami, jejichž osobní údaje jsou v držení veřejného sektoru, a dát jim jistotu, že opakované použití informací, které poskytují, bude probíhat způsobem, jenž respektuje jejich práva a zájmy (viz 14. bod odůvodnění návrhu), tj. že jejich osobní údaje nebudou neočekávaným způsobem použity proti nim. Důležitost zásady účelového omezení je jasně prokázána v souvislosti s opatřeními, která jsou zvažována pro boj proti onemocnění COVID-19, např. údaje o zdravotním stavu, které mají být zpracovávány pod kontrolou zdravotnických úřadů jako správců údajů a nesmí být použity ke komerčnímu nebo jinému účelu v rozporu s právními předpisy[32]. Subjekty veřejného sektoru, které jsou podle vnitrostátního nebo unijního práva příslušné udělit nebo odmítnout přístup pro opakované použití, musí proto vzít v úvahu, že opakované použití osobních údajů je přípustné pouze za předpokladu, že je dodržena zásada účelového omezení stanovená v čl. 5 odst. 1 písm. b) a

[31] Viz 154. bod odůvodnění, jakož i článek 86 GDPR, které zmiňují konkrétně právo Unie a členského státu týkající se přístupu veřejnosti k úředním dokumentům.
[32] Viz stanovisko EIOÚ k Evropské strategii pro data, bod 10.

článku 6 GDPR[33]. Mělo by být zamezeno jakémukoli následnému použití dat shromážděných a/nebo sdílených při plnění veřejného úkolu (např. ke zlepšení dopravy/mobility nebo k řešení závažných přeshraničních zdravotních hrozeb) pro komerční výdělečné účely (například pojištění, marketing atd.). Takové „rozšíření o neplánované funkce“ by mohlo představovat nejen porušení zásad ochrany údajů podle článku 5 GDPR, ale mohlo by také narušit důvěru fyzických osob v mechanismus opakovaného použití, který je základním cílem návrhu (viz 14. a 19. bod odůvodnění)[34].

75. V této souvislosti EDPB a EIOÚ připomínají, že čl. 6 odst. 4 GDPR objasňuje pojem „slučitelné další zpracování“ (osobních údajů). Podle definice „opakovaného použití“ uvedené v čl. 2 odst. 2 návrhu, pokud jde o osobní údaje, má být opakované použití z hlediska ochrany údajů ve skutečnosti považováno za další zpracování osobních údajů v držení subjektů veřejného sektoru pro následné, nedostatečně popsané (komerční nebo nekomerční) účely. Článek 5 návrhu, který se týká podmínek opakovaného použití, však neuvádí žádné účely, pro které může být opakované použití zákonně povoleno, ani nestanovuje, že účely jakéhokoli následného opakovaného použití musí být v souladu s čl. 6 odst. 1 písm. c) nebo e) a čl. 6 odst. 3 GDPR pečlivě určeny a jasně definovány v právních předpisech Unie nebo členského státu[35], případně musí splňovat požadavky čl. 23 odst. 1 GDPR podle čl. 6 odst. 4 GDPR[36].

76. Obecněji se jeví, že návrh nestanovuje žádnou právní povinnost subjektů veřejného sektoru zpřístupnit data, která mají v držení, k opakovanému použití, ani se výslovně nezaměřuje na ochranu cílů uvedených v článku 23 GDPR.

77. **EDPB a EIOÚ proto důrazně doporučují návrh pozměnit tak, aby bylo jasné, že opakované použití osobních údajů v držení subjektů veřejného sektoru může být povoleno, pouze pokud je zakotveno v právu Unie nebo členského státu, které stanoví seznam jasných slučitelných účelů, pro které může být další zpracování zákonně povoleno, nebo představuje nezbytné a přiměřené opatření v demokratické společnosti k zajištění cílů uvedených v článku 23 GDPR**.

78. **Kromě toho v souladu s výše uvedeným doporučením umožnit zákonný přístup k osobním údajům „uživatelům dat“, jak je uvedeno v definici „uživatelů dat“ podle čl. 2 odst. 6 návrhu, musí subjekty veřejného sektoru, které jsou podle vnitrostátního nebo unijního práva příslušné k udělení nebo odmítnutí takového přístupu pro opakované použití, vycházet z vhodného právního základu podle článku 6 GDPR použitelného na uvedené zpřístupnění. Tento aspekt však není upřesněn v článku 5**

---

[33] V této souvislosti viz 52. bod odůvodnění směrnice o otevřených datech.
[34] Viz stanovisko EIOÚ k Evropské strategii pro data, bod 25.
[35] Podle čl. 6 odst. 3 GDPR by měly právní předpisy Unie nebo členského státu na základě čl. 6 odst. 1 písm. c) nebo čl. 6 odst. 1 písm. e) GDPR určit kromě jiných prvků „účelové omezení“ zpracování osobních údajů, jakož i „účel tohoto poskytování“.
[36] V jiném ohledu zahrnutí dat v držení subjektů veřejného sektoru, která jsou chráněna z důvodu statistické důvěrnosti, do oblasti působnosti kapitoly II návrhu, v souladu s čl. 3 odst. 1 písm. b) a navzdory zásadě uvedené v čl. 3 odst. 3, představuje riziko, že budou porušeny základní zásady ochrany údajů ve statistickém odvětví, a zejména zásada účelového omezení, která přísně zakazuje používat důvěrné údaje pro účely, které nejsou výlučně statistickými, a oslabují tak důvěru fyzických osob, když poskytují své osobní údaje pro statistické účely (viz 27. bod odůvodnění výše uvedeného nařízení (ES) č. 223/2009 o evropské statistice a čl. 4 odst. 1 a čl. 4 odst. 2 doporučení Rady Evropy č. R (97)18 o ochraně osobních údajů shromažďovaných a zpracovávaných pro statistické účely).

návrhu, který se týká podmínek opakovaného použití osobních údajů v držení subjektů veřejného sektoru.

79. Ve skutečnosti 11. bod odůvodnění návrhu a odpovídající čl. 5 odst. 3 až 6 neodkazují na právo Unie nebo členského státu, které by poskytovalo právní základ podle čl. 6 odst. 1 písm. c) nebo e) GDPR, nýbrž stanoví toto (zvýraznění doplněno): „*Zejména osobní údaje by měly být předány třetí straně k opakovanému použití pouze tehdy, umožňuje-li toto předání právní základ*.“ V této souvislosti je třeba poznamenat, že by měl být uveden odkaz na právní základ „podle GDPR“. Kromě toho se uvedený bod odůvodnění omezuje pouze na vyjádření, že „*[s]ubjekty veřejného sektoru by měly případně usnadnit opakované použití dat na základě souhlasu subjektů údajů či svolení právnických osob, pokud jde o opakované použití dat, která se jich týkají, a to prostřednictvím náležitých technických prostředků. V tomto ohledu by subjekt veřejného sektoru měl podpořit další potenciální uživatele při vyžadování tohoto souhlasu tím, že zavede technické mechanismy, které umožňují předávání žádostí o souhlas od dalších uživatelů, je-li to prakticky proveditelné. Neměly by být poskytnuty kontaktní údaje, jež dalším uživatelům umožňují přímo kontaktovat subjekty údajů nebo společnosti*“.

80. Znění 14. bodu odůvodnění návrhu rovněž není jasné z hlediska stanovení vzájemného vztahu této kapitoly návrhu a GDPR: „*[…] Měly by být tudíž zavedeny dodatečné záruky pro případy, kdy je opakované použití těchto dat veřejného sektoru založeno na zpracovávání dat mimo veřejný sektor. Tyto dodatečné záruky by bylo možné spatřovat v požadavku, aby v případě předání těchto dat do třetích zemí subjekty veřejného sektoru plně zohledňovaly práva a zájmy fyzických a právnických osob (zejména ochranu osobních údajů, obchodně citlivých údajů a ochranu práv duševního vlastnictví)*“[37].

81. **EDPB a EIOÚ si dále všímají, že čl. 5 odst. 6 návrhu stanoví: „Pokud opakované použití dat nelze umožnit v souladu s povinnostmi stanovenými v odstavcích 3 až 5 a neexistuje žádný jiný právní základ pro předání dat podle nařízení (EU) 2016/679 […]“ V této souvislosti zastávají EDPB a EIOÚ názor, že podmínky uvedené v odstavcích 3 až 5 (mezi nimiž je přístup a opakované použití dat v bezpečném zpracovatelském prostředí) nelze považovat za alternativu k právnímu základu uvedenému ve vyčerpávajícím seznamu v článku 6 GDPR, pokud ve výše uvedených odstavcích není uveden odkaz na právo (Unie nebo) členského státu[38].**

82. Kromě toho není jasné, jakou úlohu má subjekt veřejného sektoru při podpoře dalších uživatelů při získávání souhlasu s opakovaným použitím subjektem údajů. K čl. 5 odst. 6 návrhu EDPB a EIOÚ dále podotýkají, že toto ustanovení zavádí povinnost subjektů veřejného sektoru („podpoří“), jejíž obsah není přesně definován. Pro větší upřesnění by měl být uveden právní základ podle GDPR pro kontaktování subjektů údajů za účelem získání jejich souhlasu s opakovaným použitím, jakož i příslušná odpovědnost související se získáním platného souhlasu podle článku 7 GDPR[39]. V této souvislosti by měla být též vzata v úvahu zjevná nerovnováha sil, která se často vyskytuje ve vztahu mezi subjektem

[37] EDPB a EIOÚ navíc poznamenávají, že subjekty veřejného sektoru by měly nejen zohledňovat, ale také **dodržovat** právní rámec chránící práva a zájmy subjektů údajů.
[38] V zájmu jasnosti by rovněž mohlo být vhodné upřesnit, že práva duševního vlastnictví uvedená v čl. 5 odst. 7 neumožňují (nepředstavují právní základ) zpracování osobních údajů.
[39] Byl by za to odpovědný subjekt veřejného sektoru, nebo další uživatel?

údajů a veřejnými orgány[40]. V tomto kontextu EDPB a EIOÚ v souladu se zásadou odpovědnosti podle GDPR připomínají, že výběr vhodného právního základu pro zpracování osobních údajů, jakož i prokázání toho, že zvolený právní základ (v tomto případě souhlas) může být oprávněně uplatněn, je v gesci správce údajů.

83. **V souladu se zásadou zákonnosti stanovenou v GDPR proto EDPB a EIOÚ důrazně doporučují vyjasnit v podmínkách opakovaného použití stanovených v článku 5 návrhu, že v právních předpisech Unie nebo členského státu musí být uveden vhodný právní důvod podle GDPR a musí být pečlivě určen subjekty veřejného sektoru, pokud jde o jakékoli následné opakované použití osobních údajů.**

84. Dalšími klíčovými prvky pro budování úrovně důvěry, na které se návrh zaměřuje, jsou zásady korektnosti a transparentnosti. Podle těchto zásad si fyzické osoby musí být plně vědomy toho, zda se osobní údaje, které poskytují subjektům veřejného sektoru nebo které jsou týmiž subjekty dále zpracovávány při plnění jejich veřejných úkolů, stanou předmětem opakovaného použití a pro jaké účely, ale musí být informovány také o příjemcích nebo kategoriích příjemců, kterým budou osobní údaje zpřístupněny, s přihlédnutím k tomu, že ve většině případů jsou subjekty údajů podle vnitrostátních právních předpisů nuceny poskytovat své osobní údaje veřejným subjektům z důvodu zákonných povinností nebo proto, že žádají o veřejné opatření nebo veřejnou službu[41].

85. Mezi podmínkami pro opakované použití stanovenými v článku 5 návrhu však nejsou uvedeny povinnosti subjektů veřejného sektoru informovat subjekty údajů podle GDPR ani nutnost zapojit je do procesu umožnění opakovaného použití jejich osobních údajů. To nejen narušuje zásady korektnosti a transparentnosti stanovené GDPR, které mají zajistit, aby fyzické osoby měly jasný přehled a kontrolu nad možnými použitími jejich osobních údajů, ale je to i v rozporu se stejnými cíli návrhu, který má zvýšit důvěru subjektů údajů, že se opakované použití „uskuteční způsobem, jenž respektuje jejich práva a zájmy“[42]. **EDPB a EIOÚ proto doporučují v návrhu uvést výslovný odkaz na povinnosti subjektů veřejného sektoru informovat subjekty údajů podle GDPR, aby se podpořil výkon práv, která jim přiznávají právní předpisy o ochraně údajů, zejména právo vznést námitku podle článku 21 GDPR. V této souvislosti EDPB a EIOÚ rovněž doporučují, aby v návrhu byly definovány vhodné prostředky, jimiž se mohou fyzické osoby otevřeným způsobem založeným na spolupráci účastnit procesu umožňujícího opakované použití jejich osobních údajů.**

86. K dosažení přiměřené úrovně důvěry v mechanismus opakovaného použití musí subjekty veřejného sektoru, které jsou podle vnitrostátního nebo unijního práva příslušné povolit přístup k opakovanému použití, dodržovat zásady minimalizace údajů a zohledňovat zvláštní ochranu požadovanou pro konkrétní odvětví, která obvykle nakládají se zvláštními kategoriemi osobních údajů, například zdravotnictví, když stanovují rozsah a podmínky pro umožnění přístupu k opakovanému použití. Při přijímání těchto rozhodnutí by měla být pečlivě zvážena přesnost, omezení uložení, integrita a důvěrnost osobních údajů, jakož i případný dopad na dotčené subjekty údajů.

---

[40] Rovněž by se mělo připomenout, že ve většině případů není souhlas vhodným právním základem pro činnosti zpracování, které vykonávají veřejné orgány. Viz Pokyny EDPB č. 5/2020 k souhlasu podle nařízení 2016/679 na adrese: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_cs.

[41] Viz Soudní dvůr Evropské unie, C-201/14, *Smaranda Bara a další*, 1. října 2015, ECLI:EU:C:2015:638.

[42] Viz 14. bod odůvodnění návrhu.

87. **V této souvislosti EDPB a EIOÚ upozorňují normotvůrce na potřebu řešit při stanovování pravidel upravujících opakované použití nezbytné požadavky na ochranu osobních údajů, zejména v „citlivých odvětvích", jako je zdravotnictví, jakož i související podmínky a zvláštní záruky na ochranu údajů.**

88. Podle GDPR je klíčovým nástrojem k zajištění řádného zohlednění požadavků na ochranu údajů a přiměřené ochrany práv a zájmů fyzických osob zejména posouzení vlivu na ochranu osobních údajů, aby byla posílena jejich důvěra v mechanismus opakovaného použití. EDPB a EIOÚ proto doporučují, aby do textu návrhu bylo zahrnuto, že v případě zpracování údajů spadajících pod článek 35 GDPR musí subjekty veřejného sektoru provádět posouzení vlivu na ochranu osobních údajů [43]. Toto posouzení pomůže určit rizika a příslušné záruky na ochranu údajů pro opakované použití, které tato rizika řeší, zejména v konkrétních odvětvích, která se obvykle zabývají zvláštními kategoriemi osobních údajů. Rozhodnutí o opakovaném použití by kromě toho, že má vycházet z právních předpisů Unie nebo členského státu, zejména u některých „citlivých odvětví" (zdravotnictví, ale také doprava nebo energetické sítě), mělo být založeno na tomto posouzení, jakož i na konkrétních podmínkách pro další uživatele a konkrétních zárukách pro subjekty údajů (například objasnění rizik opětovné identifikace anonymizovaných údajů a záruk proti těmto rizikům). A konečně, výsledky takového posouzení by měly být vždy, když je to možné, zveřejněny jako další opatření zvyšující důvěru a transparentnost[44].

89. Pokud jde o podmínky opakovaného použití, čl. 5 odst. 3 návrhu stanoví, že subjekty veřejného sektoru „mohou" uložit povinnost týkající se opakovaného použití pouze předem anonymizovaných nebo pseudonymizovaných osobních údajů. To znamená, že subjekty veřejného sektoru nejsou povinny předem zpracovávat osobní údaje, aby mohly zpřístupnit dalším uživatelům pouze předem anonymizované nebo pseudonymizované osobní údaje. V důsledku toho mohou subjekty veřejného sektoru zpřístupnit dalším uživatelům dokonce i údaje, které umožňují přímou identifikaci fyzických osob, jichž se údaje týkají, pokud by poskytnutí anonymizovaných údajů „neodpovídalo potřebám dalšího uživatele"[45]. V takovém případě mohou subjekty veřejného sektoru podle čl. 5 odst. 4 návrhu povolit opakované použití osobních údajů na místě nebo na dálku v bezpečném zpracovatelském prostředí. Vzhledem k rychlému vývoji technik opětovné identifikace a k dostupnosti pokročilých výpočetních zdrojů by však normotvůrce měl vzít v úvahu, že anonymizaci, pseudonymizaci, a dokonce ani používání bezpečného prostředí nelze ve všech případech považovat za naprosto bezpečné, a to zejména z dlouhodobého hlediska.

90. V této souvislosti EDPB a EIOÚ vítají, že 11. bod odůvodnění návrhu předpokládá, že subjekt veřejného sektoru by „využití takovéhoto bezpečného zpracovatelského prostředí" „*mohl podmínit tím, že další uživatel podepíše dohodu o mlčenlivosti, která zakazuje zveřejnění jakýchkoli informací, jež další uživatel mohl získat navzdory zavedeným zárukám, ohrožující práva a zájmy třetích stran*". **EDPB a EIOÚ však rovněž doporučují zmínit tuto dohodu o zachování důvěrnosti v právním textu návrhu mezi podmínkami opakovaného použití v článku 5. Tato dohoda by měla rovněž zakázat dalším uživatelům opětovnou identifikaci jakékoli fyzické osoby, které se údaje týkají, a měla by obsahovat povinnost dalších uživatelů průběžně hodnotit rizika opětovné identifikace a oznámit jakékoli**

[43] V této souvislosti viz 53. bod odůvodnění směrnice o otevřených datech.
[44] Viz stanovisko EIOÚ k návrhu přepracovaného znění směrnice o opakovaném použití informací veřejného sektoru, k dispozici na adrese: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf
[45] Viz 11. bod odůvodnění návrhu.

narušení dat, které vyústí v opětovnou identifikaci dotčených fyzických osob, nejen úřadu pro ochranu osobních údajů a subjektům údajů podle článků 33 a 34 GDPR, ale také dotčenému subjektu veřejného sektoru.

91. **V každém případě EDPB a EIOÚ zdůrazňují, že anonymizace a pseudonymizace nemohou být postaveny na stejnou úroveň a subjekty veřejného sektoru by je při posuzování opakovaného použití z hlediska ochrany údajů měly posuzovat odlišně. Anonymizace ve skutečnosti představuje prostředek podpory opakovaného použití informací veřejného sektoru z hlediska přínosu k hospodářské soutěži a zároveň splňuje různé požadavky vyplývající z právních předpisů o ochraně údajů, jelikož „anonymní informace", jak jsou definovány ve 26. bodě odůvodnění GDPR, nespadají do oblasti působnosti uvedených právních předpisů. Naopak informace, které prošly pseudonymizací (která by mohla vést k opětovné identifikaci fyzickou osobou pomocí dalších informací), by měly být i nadále považovány za „osobní údaje", což vede k použití dalších opatření vyžadovaných právními předpisy o ochraně údajů, čímž se současné sníží rizika pro subjekty údajů a napomůže subjektům veřejného sektoru a dalším uživatelům plnit povinnosti v oblasti ochrany údajů (zejména zásady záměrné a standardní ochrany údajů a minimalizace údajů). Tyto úvahy se vztahují též na opatření předpokládaná v čl. 5 odst. 4 návrhu, která mohou subjekty veřejného sektoru uložit jako podmínky pro opakované použití.**

3.3.3 Ustanovení čl. 5 odst. 11: opakované použití „vysoce citlivých" neosobních údajů

92. V čl. 5 odst. 11 se zavádí pojem neosobních údajů, které jsou podle unijního práva „vysoce citlivé" z hlediska předání do třetích zemí. V 19. bodě odůvodnění návrhu je uvedeno několik příkladů: „v oblasti zdraví by mohly být jako vysoce citlivé údaje o zdravotním stavu určeny určité soubory údajů v držení subjektů působících v systému veřejného zdravotnictví, jako jsou veřejné nemocnice", „například v rámci evropského prostoru pro data z oblasti veřejného zdraví nebo jiných odvětvových právních předpisů". Pokud jde o takové neosobní údaje, Komise přijme akty v přenesené pravomoci, které stanoví zvláštní podmínky vztahující se na předávání těchto údajů do třetích zemí.

93. V této souvislosti EDPB a EIOÚ upozorňují, že i když informace v anonymizovaném souboru údajů nepředstavují riziko přímé identifikace nebo vyčlenění fyzické osoby, mohlo by to v případě jejich spojení s jinými dostupnými informacemi představovat riziko nepřímé identifikace, a je tudíž pravděpodobné, že spadají do rozsahu definice osobních údajů. Čím více informací bude k dispozici a čím více údajů bude opakovaně použito a sdíleno, tím obtížnější bude v průběhu času zajistit anonymizaci[46]. V důsledku toho by EDPB a EIOÚ chtěli upozornit na skutečnost, že většina dat, která jsou již dnes – a v budoucnu budou stále více – generována a zpracovávána technikami umělé inteligence, strojového učení, internetu věcí, cloud computingu a analýzy dat velkého objemu, často spadá do oblasti definice osobních údajů. V tomto scénáři **EDPB a EIOÚ vyzývají normotvůrce, aby zvážil, že i opakované použití neosobních „vysoce citlivých" údajů předpokládané v návrhu může mít dopad na ochranu osobních údajů, zejména pokud jsou tyto neosobní údaje výsledkem**

[46] V této souvislosti viz stanovisko č. 5/2014 pracovní skupiny zřízené podle článku 29 k technikám anonymizace (WP 216), jakož i rozsudek ESD ze dne 19. října 2016, Patrick Breyer v. Bundesrepublik Deutschland, ve věci C-582/14, který odkazuje na 26. bod odůvodnění směrnice 95/46/ES a zkoumá právní a praktické prostředky, jimiž může být opětovná identifikace dotčena použitím dalších údajů v rukou třetích stran. Tuto záležitost dále rozvedou připravované Pokyny EDPB k anonymizaci/pseudonymizaci.

anonymizace osobních údajů, a tedy informací, které se původně týkaly fyzických osob. Ve skutečnosti i v těchto případech musí být plně zajištěna základní práva subjektů údajů na ochranu soukromí a údajů. Kromě toho EDPB a EIOÚ důrazně doporučují objasnit pojem „vysoce citlivé neosobní údaje“ alespoň na konkrétních příkladech.

3.3.4 Článek 6: poplatky za opakované použití dat

94. Pokud jde o poplatky předpokládané v článku 6 návrhu, EDPB a EIOÚ upozorňují, že směrnice o otevřených datech v 36. a 38. bodě odůvodnění, jakož i v čl. 6 odst. 1, 4 a 5 výslovně zmiňuje „náklady na anonymizaci“. Směrnice o otevřených datech stanovuje zejména výjimku z bezplatného opakovaného použití dokumentů, aby subjekty veřejného sektoru mohly dalším uživatelům účtovat přiměřené výdaje, které jim vzniknou v souvislosti s předběžným zpracováním, shrnutím a/nebo anonymizací osobních údajů nabízených k opakovanému použití v situacích, kdy by použití takových technik bylo odůvodněno s ohledem na zvýšená rizika plynoucí z nabízení těchto dat k opakovanému použití.

95. Vzhledem k tomu, že v určitých případech může být pseudonymizace nebo anonymizace informací v držení subjektů veřejného sektoru složitým, časově náročným a nákladným úkolem vyžadujícím odborné znalosti, které nemusí být vždy k dispozici, EDPB a EIOÚ doporučují zahrnout do čl. 6 odst. 5 návrhu, že **poplatky účtované subjekty veřejného sektoru za umožnění opakovaného použití dat mohou náležitě zohlednit náklady, které subjektům veřejného sektoru vznikly za pseudonymizaci nebo anonymizaci** osobních údajů zpřístupněných k opakovanému použití.

96. Lze také konstatovat, že **návrh mění obecnou zásadu „bezplatného“ opakovaného použití zavedenou směrnicí o otevřených datech**. Ve skutečnosti čl. 6 odst. 1 návrhu uvádí, že „*[s]ubjekty veřejného sektoru, které povolují opakované použití kategorií dat uvedených v čl. 3 odst. 1, mohou za povolení opakovaného použití těchto dat účtovat poplatky*“. V této souvislosti je tedy vzájemný vztah se směrnicí o otevřených datech nejasný.

97. Kromě toho lze podotknout, že i když čl. 6 odst. 5 uvádí, že „[p]oplatky jsou odvozeny od nákladů souvisejících s vyřízením žádostí o opakované použití (…)“, zdá se, že návrh zavádí finanční pobídky pro subjekty veřejného sektoru, aby umožnily opakované použití osobních údajů.

98. Je zapotřebí upozornit, že čl. 6 odst. 4 ukládá subjektům veřejného sektoru povinnost „*přijmou[t] opatření vybízející k opakovanému použití kategorií dat uvedených v čl. 3 odst. 1[, které obsahují osobní údaje] pro nekomerční účely a ze strany malých a středních podniků v souladu s pravidly státní podpory*“.

99. Tento aspekt, také s ohledem na kritická místa návrhu popsaná v obecných komentářích tohoto společného stanoviska, je z hlediska ochrany údajů problematický z pohledu právního i praktického provádění. Zvlášť nejasnost týkající se typu pobídek a jejich adresátů může vyvolat další otázky, zda souhlas jako jeden z právních základů, na které se odvolává čl. 5 odst. 6 návrhu, pro opakované použití

osobních údajů bude vhodným právním důvodem, zejména s ohledem na svobodu volby fyzických osob neposkytnout souhlas s opakovaným použitím jejich osobních údajů nebo jej odvolat[47].

3.3.5 Správa a institucionální aspekty: článek 7 (příslušné subjekty), článek 8 (jednotné informační místo)

100. Návrh stanoví, že členské státy budou muset zřídit jednotné kontaktní místo pro opakované použití dat veřejného sektoru (článek 8) a zřídit subjekty pověřené podporou subjektů veřejného sektoru technickými prostředky a právní pomocí související s opakovaným použitím dat veřejného sektoru (článek 7). Podle čl. 7 odst. 3 mohou být tyto „příslušné subjekty" pověřeny udělováním přístupu za účelem opakovaného použití dat, včetně osobních údajů.

101. Pokud jde o příslušné subjekty, budou tedy mimo jiné pomáhat subjektům veřejného sektoru při získávání souhlasu s opakovaným použitím nebo jeho povolení a mohou být rovněž pověřeny udělením přístupu k opakovanému použití dat v držení subjektu veřejného sektoru, včetně osobních údajů.

102. Zaprvé by z důvodu neurčitosti použité terminologie („svolení k opakovanému použití ze strany dalších uživatelů", „pro altruistické a jiné účely", „v souladu se zvláštními rozhodnutími držitelů dat") mělo být vyjasněno ustanovení čl. 7 odst. 2 písm. c). Celkový význam tohoto ustanovení („[příslušné subjekty budou] případně napomáh[at] subjektům veřejného sektoru při získávání souhlasu nebo svolení *k opakovanému použití* pro altruistické a jiné účely *ze strany dalších uživatelů*, a to v souladu se zvláštními rozhodnutími držitelů dat") je tudíž nejasný.

103. Zadruhé, přestože tyto subjekty mají v zásadě za úkol poskytovat podporu a poradenství subjektům veřejného sektoru v oblasti opakovaného použití dat, některé z jejich úkolů souvisejí s prováděním záruk stanovených v právních předpisech o ochraně údajů a podporou ochrany práv a zájmů fyzických osob s ohledem na jejich osobní údaje. Kapitola II návrhu však neobjasňuje, zda jako příslušný orgán podle článku 7 návrhu mohou být určeny dozorové úřady pro ochranu údajů, jimž nařízení GDPR uděluje též poradní pravomoci[48].

104. V této souvislosti EIOÚ a EDPB v prvé řadě zdůrazňují, že určení a navýšení počtu příslušných orgánů, které se mohou do určité míry zabývat zpracováním osobních údajů podle kapitoly II návrhu, by mohlo vytvořit skutečně složitou situaci pro subjekty veřejného sektoru, další uživatele a subjekty údajů a také by mohlo mít dopad na konzistentnost, pokud jde o monitorování toho, jak jsou uplatňována ustanovení GDPR. **Jelikož jsou tedy osobní údaje na základě návrhu předmětem opakovaného použití, EDPB a EIOÚ se domnívají, že dozorové úřady pro ochranu údajů by měly být jedinými**

[47] Jak je uvedeno v Pokynech EDPB č. 5/2020 k souhlasu podle nařízení GDPR, každý prvek nevhodného tlaku nebo vlivu na subjekt údajů (jenž se může projevovat mnoha různými způsoby), který subjektu údajů brání ve výkonu jeho svobodné vůle, učiní souhlas neplatným.

[48] Je tomu tak například v kontextu stávajících datových prostorů, jako je francouzské centrum pro data z oblasti veřejného zdraví, kde je francouzský úřad pro ochranu údajů příslušný k povolení přístupu ke konkrétním osobním údajům. V této souvislosti viz rovněž poradní pravomoci svěřené úřadům pro ochranu údajů v souvislosti s posouzením vlivu na ochranu osobních údajů, aby bylo zajištěno, že dodržují pravidla ochrany osobních údajů podle čl. 57 odst. 1 písm. l) a čl. 58 odst. 3 písm. a) GDPR.

příslušnými orgány pro dozor nad takovýmto zpracováním osobních údajů. Těmto úřadům by měly být poskytnuty vhodné zdroje, které jim umožní účinně a efektivně plnit tento úkol.

105. **Pokud by navíc byly určeny konkrétní subjekty, které budou nápomocny subjektům veřejného sektoru a dalším uživatelům dat a budou pověřeny udělováním přístupu k opakovanému použití dat, včetně osobních údajů, nesmí být tyto subjekty označovány jako „příslušné“, neboť by nejednaly jako dozorový úřad schopný sledovat a vymáhat ustanovení týkající se zpracování osobních údajů. V zájmu zajištění právní jistoty a jednotnosti uplatňování *acquis* EU v oblasti ochrany osobních údajů podléhají činnosti a povinnosti těchto určených subjektů v případě zapojení osobních údajů rovněž přímé příslušnosti a dohledu úřadů pro ochranu údajů.**

106. **Pokud jde o jejich příslušnost a úkoly podle GDPR, mají úřady pro ochranu údajů již specifické odborné znalosti v oblasti sledování souladu zpracování údajů, jakož i v oblasti zvyšování povědomí správce a zpracovatele o jejich povinnosti související se zpracováním osobních údajů. Pro zajištění souladu mezi institucionálním rámcem předpokládaným v kapitole II návrhu a GDPR proto doporučují EDPB a EIOÚ vyjasnit, že hlavními příslušnými orgány pro dohled nad ustanoveními kapitoly II týkajícími se zpracování osobních údajů a vymáhání jejich uplatňování jsou dozorové úřady pro ochranu údajů. Tyto úřady by měly úzce spolupracovat s konkrétními subjekty, které jsou podle návrhu určeny k tomu, aby pomáhaly subjektům veřejného sektoru a dalším uživatelům, a pověřeny poskytováním přístupu k opakovanému použití dat, v případě potřeby po konzultaci s dalšími příslušnými odvětvovými orgány, aby bylo zajištěno jednotné uplatňování těchto ustanovení.**

107. EDPB a EIOÚ rovněž podotýkají, že podle čl. 8 odst. 4 návrh počítá s opravným mechanismem pro další uživatele, pokud chtějí napadnout rozhodnutí o odepření přístupu k opakovanému použití, které je odlišné od rozhodnutí stanoveného ve směrnici o otevřených datech. Podle směrnice o otevřených datech (viz čl. 4 odst. 4) prostředky pro zjednání nápravy zahrnují zejména možnost přezkumu nestranným přezkumným orgánem s patřičnou odborností, jako je mimo jiné „*dozorový úřad zřízený v souladu s nařízením (EU) 2016/679 nebo vnitrostátní soudní orgán, jehož rozhodnutí jsou pro dotčený subjekt veřejného sektoru závazná*“. V této souvislosti, aniž jsou dotčeny připomínky již uvedené v tomto společném stanovisku k potřebě vyjasnit vzájemnou souhru návrhu se směrnicí o otevřených datech, upozorňují EDPB a EIOÚ normotvůrce na nesrovnalosti mezi těmito dvěma soubory pravidel.

3.4 Požadavky vztahující se na poskytovatele služby sdílení dat

Důvodová zpráva ukazuje, že „*[k]apitola III má zvýšit důvěru ve sdílení osobních a neosobních údajů a snížit transakční náklady spojené se sdílením dat mezi podniky a mezi podniky a spotřebiteli, a to vytvořením režimu oznamování pro poskytovatele služeb sdílení dat. Tito poskytovatelé budou muset plnit řadu požadavků, zejména požadavek na zachování neutrálnosti, pokud jde o vyměňovaná data. Tato data nemohou použít pro jiné účely. V případě poskytovatelů služeb sdílení dat nabízejících služby fyzickým osobám bude nutné splnit dodatečné kritérium týkající se převzetí fiduciárních povinností vůči osobám, které tyto služby využívají. Tento přístup má zajistit, aby služby sdílení dat fungovaly otevřeným způsobem založeným na spolupráci, přičemž je postavení fyzických a právnických osob posíleno tím, že jim je umožněn lepší přehled o jejich datech a větší kontrola dat. Za sledování*

dodržování požadavků spojených s poskytováním těchto služeb bude odpovídat příslušný orgán určený členskými státy“[49].

108. V čl. 9 odst. 1 návrhu, upřesněném ve 22. bodě odůvodnění, jsou stanoveny tři různé typy služeb sdílení dat:

– v písmenu a) služby zprostředkování mezi držiteli dat, jimiž jsou právnické osoby, a potenciálními uživateli dat,

– v písmenu b) služby zprostředkování mezi subjekty údajů a potenciálními uživateli dat,

– v písmenu c) „datová družstva“.

109. S ohledem na první typ služeb sdílení dat uvádí čl. 9 odst. 1 písm. a) *„služby zprostředkování mezi držiteli dat, jimiž jsou právnické osoby, a potenciálními uživateli dat, včetně poskytnutí technických či jiných prostředků umožňujících poskytování těchto služeb; tyto služby mohou zahrnovat dvoustranné či mnohostranné výměny těchto dat nebo vytváření platforem či databází umožňujících výměnu nebo společné využívání dat, jakož i zavedení zvláštní infrastruktury pro propojení držitelů dat a uživatelů dat*“.

110. Ve 22. bodě odůvodnění je uvedeno: *„Očekává se, že poskytovatelé služeb sdílení dat (zprostředkovatelé dat) budou hrát v ekonomice založené na datech klíčovou úlohu jakožto nástroj k usnadnění shromažďování a výměny značných objemů příslušných dat. Zprostředkovatelé dat nabízející služby, které spojují různé aktéry, mohou přispět k účinnému sloučení dat, jakož i k usnadnění dvoustranného sdílení dat. Specializovaní zprostředkovatelé dat, kteří jsou nezávislí jak na držitelích dat, tak na uživatelích dat, mohou hrát podpůrnou úlohu při vzniku nových ekosystémů založených na datech, jež nejsou závislé na žádném účastníkovi s významnou mírou tržní síly. Toto nařízení by se mělo vztahovat pouze na poskytovatele služeb sdílení dat, jejichž hlavním cílem je vznik obchodního, právního a případně rovněž technického vztahu mezi držiteli dat, včetně subjektů údajů, na straně jedné a potenciálními uživateli na straně druhé a napomáhání oběma stranám při transakcích týkajících se datových aktiv. Mělo by se vztahovat pouze na služby zaměřené na zprostředkování mezi neomezeným počtem držitelů dat a uživatelů dat s vyloučením služeb sdílení dat, jež mají být používány uzavřenou skupinou držitelů a uživatelů dat.“*

111. **S ohledem na výše uvedené se EDPB a EIOÚ domnívají, že otázka uvedená v obecných poznámkách tohoto společného stanoviska jako zastřešující problém, a sice riziko, že návrh vytvoří souběžný soubor pravidel, která nebudou v souladu s GDPR, je zvláště patrná s odkazem na kapitolu III návrhu. Ve skutečnosti není jasný vzájemný vztah ustanovení článku 9 návrhu, která zmiňují „držitele dat“, „potenciální uživatele dat“, „výměnu nebo společné využívání dat“, „propojení držitelů dat a uživatelů dat“, s pravidly a zásadami GDPR.**

112. Připomínáme, že služba sdílení dat jako platforma „zprostředkování mezi neomezeným počtem držitelů dat a uživatelů dat“ s vyloučením použití uzavřenou skupinou uživatelů dat, pokud se

[49] Důvodová zpráva, strana 7.

zprostředkování týká osobních údajů, je v souladu zejména se zásadou záměrné a standardní ochrany osobních údajů podle článku 25 GDPR[50].

113. EDPB a EIOÚ též upozorňují na zásady transparentnosti (a účelového omezení) zpracování osobních údajů v rámci ochrany údajů. Jak je uvedeno v pokynech pracovní skupiny zřízené podle článku 29 k transparentnosti, *„subjekt údajů by měl být schopen předem rozpoznat rozsah a důsledky zpracování“* (...) *„jinými slovy, jaký účinek bude konkrétní zpracování popsané v prohlášení/oznámení o ochraně soukromí reálně mít na subjekt údajů“*[51].

114. **Pojetí služby sdílení dat jako platformy „zprostředkování mezi neomezeným počtem držitelů dat a uživatelů dat“ jako jakéhosi tržiště s otevřenými daty by bylo v rozporu s výše uvedenými zásadami záměrné a standardní ochrany osobních údajů, transparentnosti a účelového omezení, pokud platforma neumožňuje, aby subjekt údajů zvolil účely a uživatele svých osobních údajů a dostal o nich informace předem. V zájmu jasnosti by měl návrh upřesnit tento aspekt alespoň v bodě odůvodnění.**

115. **Nejasný je také rozsah pojmu zprostředkovatel dat mezi držiteli dat a právnickými osobami, a měl by být tudíž lépe vymezen**[52].

---

[50] Viz čl. 25 odst. 2: „Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje **nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob**.“
Viz též Pokyny EDPB č. 4/2019 k zásadě záměrné a standardní ochrany soukromí na straně 20:
„Ke klíčovým koncepčním a standardním prvkům s ohledem na účelové omezení může patřit:
– Určení předem – legitimní účely musí být určeny před vytvořením návrhu zpracování.
– Specifičnost – účely musí být specifikovány a musí být výslovně uvedeny důvody pro zpracovávání osobních údajů.
–Orientace na účel – účel zpracování by měl být vodítkem při navrhování zpracování a měl by stanovit meze zpracování.
– Nezbytnost – účel určuje, které osobní údaje jsou nezbytné pro dané zpracování.
– Slučitelnost – každý nový účel musí být slučitelný s původním účelem, pro který byly údaje shromážděny, a musí být vodíkem pro relevantní změny v návrhu.
– Omezení dalšího zpracování – správce by neměl propojovat soubory údajů ani provádět žádné další zpracování pro nové, neslučitelné účely.
– Omezení opětovného použití – správce by měl používat technická opatření, včetně hašování a šifrování, aby omezil možnost použití osobních údajů pro jiné účely. Správce by měl zavést rovněž organizační opatření, jako jsou zásady a smluvní závazky, jež omezují opakované použití osobních údajů.
– Přezkum – správce by měl pravidelně přezkoumávat, zda je zpracování nezbytné pro účely, pro které byly údaje shromážděny, a provést zkoušku návrhu s ohledem na účelové omezení.“
[51] Pracovní skupina zřízená podle článku 29, Pokyny k transparentnosti podle nařízení 2016/679, WP260, rev. 01, s. 7.
[52] Ve 22. bodě odůvodnění je uvedeno: „[…] Vyloučeni by měli být poskytovatelé **cloudových služeb** stejně jako **poskytovatelé služeb, kteří získávají data od držitelů dat, data shromažďují, obohacují nebo transformují a udělují uživatelům dat licence na používání** výsledných dat, aniž by vznikl přímý vztah mezi držiteli dat a uživateli dat, jako jsou například **zprostředkovatelé reklamy nebo dat, poradenské společnosti v oblasti dat,**

116. Obecně lze poznamenat, že návrh neupřesňuje, **jak (podle kterého právního základu GDPR) budou poskytovatelé služeb sdílení dat shromažďovat osobní údaje pro účely sdílení**.

117. Není také jasné, **zda poskytovatelé služeb sdílení dat mohou zprostředkovat data, která** podle kapitoly II návrhu **mohou subjekty veřejného sektoru používat opakovaně**.

118. Z důvodu transparentnosti a za účelem zvýšení (spíše než snížení) úrovně důvěry občanů je rovněž klíčové, aby bylo v návrhu vyjasněno, že služba sdílení dat bude poskytována poté, co držitelé dat a uživatelé dat zaplatí určitou „cenu". Tento aspekt lze vyvodit ze znění čl. 11 odst. 3 návrhu[53], ale není jasný a úplný (neposkytuje jasný obrázek o peněžních transakcích provázejících zpracování osobních údajů). Jasná pobídka ke „zpeněžení" osobních údajů také zvyšuje důležitost kontrol dodržování ochrany údajů[54]. V této souvislosti, stejně jako ve vztahu k ostatním kapitolám návrhu, nebere posouzení dopadů[55] bohužel v úvahu rizika ochrany údajů.

119. EDPB a EIOÚ dále podotýkají, že návrh neposkytuje jasný obraz, například v podobě příkladů v bodech odůvodnění, o „případech použití" služeb sdílení dat (jejichž „aspekt peněžní transakce", jak je zdůrazněno, má být v takovém případě veřejnosti a dotčeným osobám objasněn). Kupříkladu 22. bod odůvodnění upřesňuje, co není platformou pro výměnu údajů, která má být považována za „zprostředkovatele dat": „*Toto nařízení by se nemělo vztahovat na platformy pro výměnu údajů, které používá výhradně jeden držitel údajů s cílem umožnit využívání údajů, které má v držení, ani na platformy vyvinuté v souvislosti s předměty a zařízeními připojenými k internetu věcí, jejichž hlavním cílem je zajistit funkčnost připojeného předmětu nebo zařízení a umožnit služby s přidanou hodnotou*", neuvádí však v této souvislosti předpokládaný případ použití.

---

poskytovatelé datových produktů vyplývajících z přidané hodnoty, kterou datům zajistil poskytovatel služby. Poskytovatelé služeb sdílení dat by měli být současně oprávněni provádět **úpravy vyměněných dat, pokud to zvyšuje použitelnost** dat ze strany uživatele dat, jestliže to uživatel dat požaduje, jako je například převod do určitých formátů. Na **služby, které se zaměřují na zprostředkování obsahu, zejména obsahu chráněného autorským právem, by se** toto nařízení **vztahovat nemělo**.
Toto nařízení by se nemělo vztahovat na **platformy pro výměnu údajů, které používá výhradně jeden držitel dat** s cílem umožnit využívání údajů, které má v držení, ani na platformy vyvinuté v souvislosti s předměty a zařízeními připojenými k internetu věcí, jejichž hlavním cílem je zajistit funkčnost připojeného objektu nebo zařízení a umožnit služby s přidanou hodnotou. „Poskytovatelé konsolidovaných obchodních informací" ve smyslu čl. 4 odst. 1 bodu 53 směrnice Evropského parlamentu a Rady 2014/65/EU, jakož i „poskytovatelé služeb informování o účtu" ve smyslu čl. 4 bodu 19 směrnice Evropského parlamentu a Rady (EU) 2015/2366 by pro účely tohoto nařízení neměli být považováni za poskytovatele služeb sdílení údajů. Na subjekty, které svou činnost omezují na snazší použití dat zpřístupněných na základě datového altruismu a které působí na neziskovém základě, by se neměla vztahovat kapitola III tohoto nařízení, neboť tato činnost slouží cílům obecného zájmu, jelikož zvyšuje objem dat, která jsou k dispozici pro tyto účely."

[53] Ustanovení čl. 11 odst. 3 návrhu uvádí: „poskytovatel zajistí, aby postup přístupu k jeho službě byl spravedlivý, transparentní a nediskriminační jak pro držitele dat, tak pro uživatele dat, a to včetně **cen**."

[54] V této souvislosti EDPB pracuje na pokynech ke shromažďování a používání osobních údajů za finanční odměnu.

[55] Posouzení dopadů doprovázející akt o správě dat, SWD(2020) 295 final, k dispozici na adrese: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0295:FIN:EN:PDF.

3.4.1 Zprostředkovatelé dat podle čl. 9 odst. 1 písm. b): služby zprostředkování mezi subjekty údajů a potenciálními uživateli dat[56].

120. EDPB a EIOÚ konstatují, že ustanovení týkající se služeb zprostředkování mezi subjekty údajů, jež chtějí zpřístupnit své osobní údaje, a potenciálními uživateli dat při výkonu práv stanovených v nařízení (EU) 2016/679 podle čl. 9 odst. 1 písm. b) se použije, aniž by bylo dotčeno účinné uplatňování práv subjektů údajů a povinností správce údajů podle GDPR.

121. Návrh však neupřesňuje způsoby, kterými by tito poskytovatelé služeb účinně pomáhali fyzickým osobám při výkonu jejich práv podle GDPR, ani neuvádí, na jaké zpracování osobních údajů by se taková pomoc přesně vztahovala a pro které uživatele dat by byla určena[57].

122. EDPB a EIOÚ se v první řadě domnívají, že účinné uplatňování práv subjektů údajů a jeho možné způsoby stanoví GDPR, pod dohledem vnitrostátních dozorových úřadů podle článku 51 téhož nařízení. Nejasnosti ohledně přesných způsobů pomoci poskytované při výkonu práv subjektů údajů, jakož i ohledně příjemců takového procesu a jejich povinností vůči subjektům údajů mohou vést k další právní nejistotě při účinném výkonu práv subjektů údajů podle GDPR.

123. **EDPB a EIOÚ by proto doporučili, aby návrh odrážel právní rámec EU (GDPR), podle něhož může Evropský sbor pro ochranu osobních údajů tyto způsoby, jakož i související povinnosti vztahující se na poskytovatele a příjemce služeb sdílení dat více upřesnit v souladu s článkem 70 GDPR[58].**

124. Není rovněž jasné, zda služby zprostředkování podle čl. 9 odst. 1 písm. b) návrhu, jejichž definice není uvedena v článku 2, odkazují na systémy pro správu osobních údajů, či nikoli, a zda odkazují pouze na ně (a v jakém rozsahu). EDPB a EIOÚ poukazují na rozdíl mezi systémy pro správu osobních údajů, které umožňují správu osobních údajů a usnadňují výkon práv subjektů údajů („propojení se subjektem údajů“)[59] na jedné straně a poskytovatelů služeb sdílení dat mezi podniky (jejichž vzájemná souvislost se „zprostředkovateli dat“ je nejasná) na straně druhé. S ohledem na posledně jmenované mohou být kritická místa z hlediska ochrany údajů významnější, pokud je subjekt údajů více vzdálen a hrozí mu, že nebude mít jasný přehled o sdílení svých osobních údajů a kontrolu nad ním[60].

---

[56] Ustanovení čl. 9 odst. 1 písm. b) návrhu uvádí: „služby zprostředkování mezi subjekty údajů, jež chtějí zpřístupnit své osobní údaje, a potenciálními uživateli dat, včetně poskytnutí technických či jiných prostředků umožňujících poskytování těchto služeb, při výkonu práv stanovených v nařízení (EU) 2016/679.“

[57] Formulace „poskytovatel nabízející služby subjektům údajů **jedná při usnadňování výkonu jejich práv v nejlepším zájmu subjektů údajů**, zejména radí
subjektům údajů ohledně možných použití dat a standardních podmínek spojených s tímto použitím;“ v čl. 11 odst. 10 návrhu je stále poměrně neurčitá.

[58] V této souvislosti EDPB v současnosti pracuje na pokynech k právům subjektu údajů.

[59] Viz stanovisko EIOÚ k systémům pro správu osobních údajů, 20. října 2016, k dispozici na adrese: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[60] Viz stanovisko EIOÚ k Evropské strategii pro data, bod 20: „EIOÚ zároveň zdůrazňuje potřebu opatrnosti, pokud jde o úlohu zprostředkovatelů dat, kteří se aktivně podílejí na shromažďování obrovských souborů dat, včetně osobních údajů z různých zdrojů. Využívají různé zdroje dat používané pro služby související s daty, například data, která jsou zveřejňována pro jiné nesouvisející účely; data z veřejných registrů (otevřená data), jakož i data „získaná automatickým procházením webových stránek“ na internetu a v sociálních médiích, často v rozporu s právními předpisy o ochraně údajů. V této souvislosti EIOÚ konstatuje, že činnosti zprostředkovatelů dat velkého objemu jsou podrobovány zvýšené kontrole a jsou vyšetřovány řadou vnitrostátních úřadů pro ochranu údajů.“

125. Ve všech případech však platí zásady transparentnosti, korektnosti a účelového omezení.

126. Ve svém stanovisku o systémech pro správu osobních údajů EIOÚ upozornil, že *„[v] každém případě je zásadní zajistit transparentnost obchodního modelu vůči fyzickým osobám, jejichž údaje se zpracovávají, aby si byly vědomy příslušných zájmů (systémů pro správu osobních údajů a dalších poskytovatelů služeb) a mohly systémy pro správu osobních údajů používat s plným vědomím“*[61].

127. Návrh poskytuje některá objasnění týkající se poskytovatelů služeb sdílení dat, kteří nejsou usazeni v Unii, s cílem určit, zda takový poskytovatel nabízí služby v Unii. Toto upřesnění ve 27. bodě odůvodnění návrhu se zdá být v souladu s 23. bodem odůvodnění GDPR. V zájmu právní jistoty by mohlo být přínosné upřesnit, že v případě zpracování osobních údajů se na výše uvedené poskytovatele služeb sdílení dat, kteří nejsou usazeni v Unii, vztahují pravidla a zásady GDPR.

3.4.2 Zprostředkovatelé dat podle čl. 9 odst. 1 písm. c): „datová družstva“

128. EDPB a EIOÚ zdůrazňují, že pojem „služba datových družstev“ zavedený v čl. 9 odst. 1 písm. c) návrhu[62] zůstává jak z hlediska povahy, tak z hlediska povinností nejasný. V této souvislosti by měla být zavedena jasná definice těchto poskytovatelů služeb sdílení dat, jakož i jejich příslušné povinnosti, aby se zamezilo jakékoli právní nejistotě při poskytování takových služeb.

129. Zatímco návrh upřesňuje, že datová družstva *„usilují o posílení postavení fyzických osob při přijímání informovaných rozhodnutí před udělením souhlasu s použitím dat, ovlivňují podmínky organizací uživatelů dat spojené s použitím dat nebo případně řeší spory mezi členy skupiny ohledně možného způsobu použití dat, pokud se tato data týkají několika subjektů údajů v rámci této skupiny“*[63], je třeba připomenout, že povinnosti transparentnosti, jakož i podmínky pro platný souhlas subjektu údajů podle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679 a podmínka pro zpracování osobních údajů podle tohoto právního základu jsou definovány a stanoveny v témže nařízení.

130. **EDPB a EIOÚ se proto domnívají, že postavení fyzických osob při přijímání informovaných rozhodnutí nebo řešení případného sporu o tom, jak lze data použít, nelze považovat za**

---

[61] Viz strana 13 bod 52 stanoviska EIOÚ k systémům pro správu osobních údajů, 20. října 2016, k dispozici na adrese: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.
Viz též bod 53, strana 13: *„Zdá se, že model systémů pro správu osobních údajů vyzývá k debatě o tom, kdo naše osobní údaje „vlastní“. Fyzické osoby v EU mají základní právo na ochranu svých osobních údajů na základě článku 8 Listiny základních práv EU. Podrobná práva a povinnosti spojené s výkonem tohoto práva jsou podrobněji upraveny v nedávno přijatém GDPR. Tyto otázky nejsou specifické pro systémy pro správu osobních údajů: osobní údaje jsou často vnímány jako „měna“, kterou platíme za tzv. „bezplatné“ služby na internetu. Tento trend však neznamená, že osobní údaje fyzických osob lze legálně považovat za majetek, s nímž lze volně obchodovat jako s jakýmkoli jiným majetkem na trhu. Naopak, systémy pro správu osobních údajů v zásadě nebudou moci „prodávat“ osobní údaje, ale jejich úlohou bude spíše umožnit třetím stranám používat osobní údaje pro **konkrétní účely** a **konkrétní časové období**, v souladu s **podmínkami, které určí samotné fyzické osoby**, a **veškerými dalšími zárukami, které poskytují příslušné právní předpisy o ochraně údajů**.“*

[62] Ustanovení čl. 9 odst. 1 písm. c) návrhu zmiňuje „služby datových družstev, tj. služby podporující subjekty údajů nebo jednočlenné společnosti či mikropodniky, malé a střední podniky, jež jsou členy družstva nebo **které pověří družstvo sjednáním podmínek pro zpracování údajů před udělením souhlasu,** při **přijímání informovaných rozhodnutí před udělením souhlasu se zpracováním údajů,** a **umožňující mechanismy pro výměnu názorů na účely zpracování dat a podmínky, jež by nejlépe reprezentovaly zájmy subjektů údajů nebo právnických osob**“.

[63] Ustanovení 24. bodu odůvodnění návrhu.

vyjednatelné podmínky, ale spíše za povinnosti správců údajů podle nařízení (EU) 2016/679. V této souvislosti je rovněž třeba zdůraznit, že odkaz na data, která by se „týkala" několika subjektů údajů, pokud jde o osobní údaje, uvedený ve 24. bodě odůvodnění návrhu, nemusí být v souladu s definicí osobních údajů podle nařízení (EU) 2016/679[64], která uvádí „veškeré informace o identifikované nebo identifikovatelné fyzické osobě".

131. Navíc, jak připomíná 24. bod odůvodnění návrhu, *„práva podle nařízení (EU) 2016/679 mohou uplatňovat pouze jednotlivé fyzické osoby a nemohou být svěřena nebo udělena datovému družstvu"*. EDPB a EIOÚ se domnívají, že vyjádření takových zásad s možností, aby datová družstva byla pověřena „sjednáním podmínek pro zpracování údajů před udělením souhlasu", je přinejmenším nejasné, ne-li přímo rozporuplné. Ve skutečnosti jsou „podmínky" zpracování osobních údajů – v podstatě – shodné s těmi, které jsou zakotveny v GDPR, a nelze je tudíž upravit ani nahradit smlouvou nebo jiným typem soukromého ujednání.

3.4.3 Článek 10: režim oznamování – obecné požadavky na způsobilost k registraci – obsah oznámení; výsledek (a načasování) oznámení. Článek 11: podmínky pro poskytování služeb sdílení dat

132. Kapitola III návrhu stanovuje povinnost poskytovatele služeb sdílení dat podle čl. 9 odst. 1 předložit oznámení příslušnému orgánu (povinné oznámení). V čl. 10 odst. 1 a 2 jsou stanovena pravidla pro určení příslušnosti členského státu pro účely návrhu. Jedná se o příslušnost členského státu, v němž je hlavní provozovna poskytovatele služeb sdílení dat, nebo členského státu, v němž je usazen právní zástupce poskytovatele služeb sdílení dat, který není usazen v Unii.

133. Informace, které mají být uvedeny v oznámení, jsou stanoveny v čl. 10 odst. 6 písm. a) až h) návrhu[65]. Kromě toho čl. 10 odst. 7 stanovuje, že *„[n]a žádost poskytovatele vydá příslušný orgán do jednoho týdne standardizované prohlášení potvrzující, že poskytovatel podal oznámení podle odstavce 4*".

134. Režim oznamování, na který poukazuje důvodová zpráva, „spočívá *v oznamovací povinnosti s následným sledováním plnění požadavků při výkonu činností příslušnými orgány členských států*"[66]. Tento aspekt je však upřesněn ve 30. a 31. bodě odůvodnění návrhu[67].

---

[64] Definice podle čl. 4 odst. 1 GDPR.

[65] „Oznámení obsahuje tyto informace:
a) jméno poskytovatele služeb sdílení dat;
b) právní postavení, právní formu a registrační číslo poskytovatele, je-li registrován v obchodním rejstříku nebo jiném podobném veřejném rejstříku;
c) adresu hlavní provozovny poskytovatele v Unii, pokud existuje, a případně i jakékoli vedlejší pobočky v jiném členském státě nebo právního zástupce ustanoveného podle odstavce 3;
d) případně internetové stránky, na nichž jsou uvedeny informace o poskytovateli a jeho činnosti;
e) kontaktní osoby a kontaktní údaje poskytovatele;
f) popis služby, kterou poskytovatel hodlá poskytovat;
g) předpokládané datum zahájení činnosti;
h) členské státy, v nichž poskytovatel hodlá služby poskytovat."

[66] Důvodová zpráva, strana 5.

[67] „(30) Pro služby sdílení dat je třeba zavést oznamovací postup, aby byla v Unii zajištěna správa dat, která je založená na důvěryhodné výměně dat. Přínosů plynoucích z důvěryhodného prostředí by bylo nejlépe dosaženo

135. „Prověřování“ poskytovatele služeb sdílení dat se proto omezuje na ověření (převážně formálních) požadavků stanovených v článku 10 příslušným orgánem a proběhne ve velmi krátké lhůtě (jeden týden od data oznámení).

136. **V této souvislosti EDPB a EIOÚ poznamenávají, že režim „prověřování“ je téměř „deklarativní“ a že Komise zvolila „nejuvolněnější“ režim (na rozdíl například od režimu oprávnění). EDPB a EIOÚ podotýkají, že přinejmenším v souvislosti se zpracováním osobních údajů by režim měl více chránit (tj. měl by zajišťovat více kontrol a záruk pro subjekty údajů, včetně zásadně důležitých aspektů ochrany údajů). To by rovněž umožnilo zajistit vyšší úroveň důvěry, na kterou se Komise zaměřuje.**

137. **V zájmu řešení tohoto problému by měl být změněn zejména 31. bod odůvodnění návrhu.**

138. V souladu se zásadou odpovědnosti při ochraně údajů jsou poskytovatelé služeb sdílení dat mimo jiné schopni prokázat, že zavádějí zásady a postupy, které subjektům údajů umožňují snadno vykonávat jejich individuální práva na ochranu údajů (postupy k zajištění souladu s právy subjektů údajů), a měli by dokumentovat rozhodnutí o sdílení dat (zejména včetně účelů, pro které budou osobní údaje sdíleny, a příjemců nebo kategorií příjemců, jimž budou sděleny), dokazující, že dodržují právní předpisy o ochraně údajů[68]. Tyto aspekty (které by měly tvořit „jádro“ označování předpokládaného v návrhu[69]) povedou k vytvoření větší důvěry veřejnosti v poskytovatele služeb sdílení dat.

139. EDPB a EIOÚ rovněž poznamenávají, že na poskytování služeb sdílení dat, stanovené v článku 11, se vztahují podmínky uvedené v odstavcích 1 až 11. V této souvislosti EDPB a EIOÚ konstatují, že i když se mezi podmínkami zmiňuje dodržování pravidel hospodářské soutěže (podle odstavce 9), tyto (vyčerpávajícím způsobem uvedené) podmínky nezahrnují dodržování pravidel ochrany údajů.

140. **S ohledem na výše uvedené prvky a vzhledem k možnému riziku pro subjekt údajů při zpracování osobních údajů, které mohou nést poskytovatelé služeb sdílení dat, se EDPB a EIOÚ domnívají, že režim deklaratorního oznamování podle návrhu nestanoví dostatečně přísný postup prověřování**

---

uložením řady požadavků na poskytování služeb sdílení dat, **aniž by se však vyžadovalo výslovné rozhodnutí či správní akt přijatý příslušným orgánem v souvislosti s poskytováním těchto služeb**.
(31) Na podporu účinného přeshraničního poskytování služeb by se mělo vyžadovat, aby poskytovatel služeb sdílení dat **zaslal oznámení pouze určenému příslušnému orgánu z členského státu, kde se nachází jeho hlavní provozovna nebo jeho právní zástupce**. Toto **oznámení by nemělo znamenat více než pouhé prohlášení o záměru poskytovat takovéto služby a mělo by uvádět pouze informace stanovené v tomto nařízení**.“ (zvýraznění doplněno)

[68] Podle článku 30 GDPR: „Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace: a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů; b) účely zpracování; c) popis kategorií subjektů údajů a kategorií osobních údajů; d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích; e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk; f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů; g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1. […]“

[69] Posouzení dopadů návrhu se týká označování nebo certifikace, mimo jiné na straně 19: „[v]zájemné uznávání mechanismů certifikace/označování a režimů důvěryhodnosti pro datový altruismus umožní shromáždit a použít údaje v nezbytném rozsahu“; na straně 25: „rámec pro certifikaci/označování pro zprostředkovatele dat“; na straně 26: „Rámec pro certifikaci nebo označování by umožnil novým zprostředkovatelům dat zviditelnit se více jako důvěryhodní organizátoři / subjekty připravující sdílení nebo sloučení dat.“

použitelný na tyto služby. EDPB a EIOÚ doporučují prozkoumat alternativní postupy, které by zejména měly zohlednit systematičtější zahrnutí nástrojů odpovědnosti a dodržování předpisů pro zpracování osobních údajů podle GDPR, zejména dodržování kodexu chování nebo mechanismu pro vydávání osvědčení.

141. Lze též podotknout, že s ohledem na poskytovatele služeb sdílení dat návrh nepředpokládá záruky stanovené v kapitole IV návrhu pro organizace pro datový altruismus (článek 18, požadavky na transparentnost; článek 19, zvláštní požadavky), a to navzdory možnému dopadu těchto služeb sdílení dat na práva a svobody dotčených osob.

142. Tento rozdíl mezi těmito dvěma režimy oznamování by mohl vést k výkladu *a contrario*, tedy že se požadavky stanovené pro organizace pro datový altruismus a týkající se ochrany osobních údajů v případech, kdy jsou zpracovávány osobní údaje (například informování držitelů dat o jakémkoli zpracování mimo Unii[70]), nevztahují na poskytovatele služeb sdílení dat.

143. **V této souvislosti EDPB a EIOÚ konstatují, že organizace zapojené do ujednání o „sloučení dat" nebo sdílení dat by měly dodržovat určité společné normy, dohled nad nimiž ze strany nezávislých úřadů pro ochranu údajů návrh výslovně připomíná, a to nejen v souvislosti s podmínkami interoperability, ale také s podmínkami pro zajištění zákonnosti zpracování osobních údajů a usnadnění výkonu práv subjektů údajů (např. prostřednictvím ujednání o společných správcích podle článku 26 GDPR).**

144. EDPB a EIOÚ navíc konstatují, že návrh zmiňuje scénáře (použití metadat pro rozvoj služby sdílení dat podle čl. 11 odst. 2; kontinuita přístupu držitelů dat a uživatelů dat k datům uloženým poskytovatelem sdílení dat po platební neschopnosti poskytovatele sdílení dat podle čl. 11 odst. 6), které je zapotřebí upřesnit, aby byly uvedeny do souladu s pravidly a zásadami ochrany osobních údajů.

145. EDPB a EIOÚ rovněž podotýkají, že připomínky vznesené na základě obecných poznámek tohoto stanoviska, které se týkají definic použitých v návrhu a otázky právního základu podle GDPR pro zpracování osobních údajů, jsou relevantní i s ohledem na ustanovení kapitoly III návrhu.

146. Dále s konkrétním odkazem na cíl zajistit lepší kontrolu přístupu a používání osobních údajů subjektem údajů připomínáme, že zásada účelového omezení má zvláštní význam s ohledem na zprostředkovatele dat mezi podniky. Ustanovení 26. bodu odůvodnění návrhu[71], který, jak se zdá, ztotožňuje účel zpracování osobních údajů se zprostředkováním při sdílení údajů, a to bez dalšího upřesnění, může vzbuzovat obavy z hlediska ochrany údajů[72].

---

[70] Ustanovení čl. 19 odst. 1 písm. b) návrhu.

[71] Ustanovení 26. bodu odůvodnění návrhu: „Klíčovým prvkem k zajištění důvěry a větší kontroly ze strany držitele dat a uživatelů dat v rámci služeb sdílení dat je neutralita poskytovatelů služeb sdílení dat, pokud jde o data vyměňovaná mezi držiteli dat a uživateli dat. Je proto nezbytné, aby poskytovatelé služeb sdílení dat **jednali pouze jako zprostředkovatelé** v rámci transakcí a nepoužívali vyměňovaná data k **jinému účelu**. […]"

[72] Viz rovněž čl. 2 odst. 4 návrhu: „‚metadaty' [se rozumí] shromážděná data o jakékoli činnosti fyzické nebo právnické osoby **za účelem poskytování služby sdílení dat**"; Ustanovení čl. 2 odst. 7: „‚sdílením dat' [se rozumí] poskytování dat uživateli dat jejich držitelem za **účelem společného či individuálního použití sdílených dat**"; Ustanovení čl. 11 odst. 1: „poskytovatel nesmí použít data, pro něž poskytuje služby, k **jiným účelům, než je možnost uživatelů dat nakládat s nimi**".

147. EDPB a EIOÚ se domnívají, že poznámky uvedené v oddíle 3.3 tohoto společného stanoviska týkající se opakovaného použití osobních údajů v držení subjektů veřejného sektoru jsou rovněž relevantní s ohledem na služby sdílení dat:

– musí být přesně definovány rozsah a účel jakéhokoli sdílení osobních údajů nebo přístupu k nim, které musí probíhat plně v souladu s GDPR, s přihlédnutím k požadavkům zákonnosti, účelového omezení a oprávněného očekávání subjektů údajů,

– mělo by být jasné, že každý „aktér" řetězce zpracování údajů, včetně poskytovatele služeb sdílení dat a uživatele či uživatelů, poskytne subjektům údajů informace podle článků 13 a 14 GDPR (často bude příslušným ustanovením GDPR v tomto kontextu článek 14, který je použitelný v případě, že osobní údaje nezískal subjekt údajů). V této souvislosti doporučujeme dodat, že poskytovatel služeb sdílení dat poskytne subjektu údajů uživatelsky přívětivé nástroje, které mu poskytnou komplexní přehled o tom, jak jsou jeho osobní údaje sdíleny, jakož i uživatelsky přívětivý nástroj pro odvolání souhlasu v případě, že poskytovanou službu tvoří nástroj k získání souhlasu subjektů údajů se zpracováním jejich osobních údajů podle čl. 11 odst. 11 návrhu,

– posouzení vlivu na ochranu osobních údajů je klíčovým nástrojem k zajištění řádného zohlednění požadavků na ochranu údajů a přiměřené ochrany práv a zájmů fyzických osob, aby se zvýšila jejich důvěra v mechanismus pro opakované použití. EDPB a EIOÚ proto doporučují, aby bylo do textu návrhu zahrnuto, že **posouzení vlivu na ochranu osobních údajů musí poskytovatelé služeb sdílení dat (a uživatel dat) provádět v případě, že zpracování údajů spadá pod článek 35 GDPR**. Sdílení údajů předpokládané v návrhu může ve skutečnosti zahrnovat rozsáhlé zpracování, které kombinuje data z různých zdrojů, kam případně patří zvláštní kategorie dat a/nebo osobní údaje zranitelných skupin subjektů údajů. V takovém případě mají správci údajů povinnost provést posouzení vlivu na ochranu osobních údajů v souladu s článkem 35 GDPR. Kromě toho, kdykoli je to možné, poskytovatel služeb sdílení dat, jakož i uživatel(é) zveřejní výsledky takových posouzení, a to jako opatření ke zvýšení důvěry a transparentnosti.

3.4.4 Články 12 a 13: příslušné orgány a sledování souladu (s články 10 a 11)

148. Ustanovení čl. 12 odst. 3 návrhu uvádí, že *„[u]rčené příslušné orgány, orgány pro ochranu údajů, vnitrostátní orgány pro hospodářskou soutěž, orgány pověřené kybernetickou bezpečností a ostatní dotčené odvětvové orgány si vyměňují informace, které jsou nezbytné pro plnění jejich úkolů ve vztahu k poskytovatelům služeb sdílení dat"*.

149. Toto znění připisuje úřadům pro ochranu údajů ještě menší úlohu než znění použité v návrhu ve vztahu k organizacím pro datový altruismus[73], které odkazuje na *„spolupráci s úřady pro ochranu údajů"*.

[73] Ustanovení čl. 20 odst. 3: „Příslušný orgán plní své úkoly [orgánu odpovědného za rejstřík uznávaných **organizací pro datový altruismus** a za sledování souladu s požadavky kapitoly IV návrhu] **ve spolupráci s úřadem pro ochranu údajů**, pokud tyto úkoly souvisejí se zpracováváním osobních údajů, a s příslušnými odvětvovými orgány v témže členském státě. V případě jakýchkoli **otázek vyžadujících posouzení souladu s nařízením (EU)**

150. V této souvislosti, jak je zdůrazněno v oddíle 3.7 tohoto společného stanoviska, EDPB a EIOÚ připomínají, že mnoho ustanovení této kapitoly, jakož i ostatních kapitol návrhu se týká zpracování osobních údajů a že orgány pro ochranu údajů jsou orgány „ústavně“ příslušnými pro dohled nad ochranou osobních údajů podle článku 8 Listiny a článku 16 SFEU.

151. S ohledem na článek 13 návrhu upravující sledování souladu, bez ohledu na 28. bod odůvodnění, v němž se uvádí, že návrhem by neměla být dotčena odpovědnost dozorových úřadů za zajištění souladu s GDPR, mají EDPB a EIOÚ za to, že by správa a sledování souladu měly být lépe definovány, aby se zajistilo vhodnější prověřování poskytovatelů služeb sdílení dat (a organizací pro datový altruismus), včetně souladu s GDPR; a aby bylo zároveň zamezeno jakémukoli překrývání nebo konfliktu v oblasti příslušnosti mezi orgány zřízenými podle návrhu (které podle znění čl. 12 odst. 3 – a čl. 20 odst. 3 – nejsou úřady pro ochranu údajů) a úřady pro ochranu údajů.

152. **EDPB a EIOÚ se tudíž domnívají, že takovouto lepší definici správy by zajistilo určení orgánů pro ochranu údajů jako hlavních příslušných úřadů pro sledování souladu a dohled nad dodržováním ustanovení kapitoly III návrhu.**

153. Určení úřadů pro ochranu údajů jako hlavních příslušných úřadů pro dohled nad ustanoveními kapitoly III návrhu a jejich vymáhání by rovněž zajistilo jednotnější regulační přístup napříč členským státem, a přispělo by tak k důslednému uplatňování návrhu. Pokud jde o jejich příslušnost a úkoly podle GDPR, úřady pro ochranu údajů již mají specifické odborné znalosti v oblasti sledování souladu zpracování údajů, auditu konkrétních činností zpracování údajů a sdílení dat, posouzení vhodných opatření k zajištění vysoké míry bezpečnosti uchovávání a přenosu osobních údajů, jakož i v oblasti zvyšování povědomí správců a zpracovatelů o jejich povinnosti související se zpracováním osobních údajů.

154. Určení úřadů pro ochranu údajů jako hlavního příslušného orgánu pro dohled a vymáhání ustanovení podle kapitoly III se podpoří předpokládaným ustanovením podle čl. 12 odst. 3, které s cílem zajistit soudržné uplatňování těchto ustanovení umožňuje výměnu informací mezi úřady pro ochranu údajů, vnitrostátními orgány pro hospodářskou soutěž, orgány odpovědnými za kybernetickou bezpečnost a dalšími příslušnými odvětvovými orgány.

155. EDPB a EIOÚ se navíc domnívají, že při sledování souladu nelze pravomoc příslušných orgánů omezit na „oprávnění vyžádat si informace“, jak vyplývá z čl. 13 odst. 2 návrhu. Toto omezení rozhodně pramení z deklaratorní povahy „režimu označování“ předpokládaného návrhem, i když neodpovídá úrovni prověřování, kterou označování vyžaduje, a to vzhledem k vysokým očekáváním ohledně souladu ochrany údajů vyplývajícím z takového označování, zejména vůči subjektům údajů.

156. V neposlední řadě EDPB a EIOÚ zdůrazňují, že úřadům pro ochranu údajů by měly být poskytnuty odpovídající zdroje, aby mohly účinně a efektivně vykonávat nezbytný dohled.

2016/679 si příslušný orgán nejprve vyžádá stanovisko nebo rozhodnutí příslušného dozorového úřadu zřízeného podle zmíněného nařízení a tímto stanoviskem či rozhodnutím se řídí.“
Je zapotřebí také poznamenat, že 28. bod odůvodnění – s ohledem na **poskytovatele služeb sdílení dat** – upřesňuje, že „[t]ímto nařízením **by neměla být dotčena** povinnost poskytovatelů služeb sdílení dat dodržovat nařízení (EU) 2016/679 a **odpovědnost dozorových úřadů za zajištění souladu s tímto nařízením**“. Stejný požadavek **není** uveden v souvislosti s organizacemi pro datový altruismus.

3.5 Altruismus v oblasti dat

3.5.1 Vzájemný vztah mezi datovým altruismem a souhlasem podle nařízení GDPR

157. Pojem „datový altruismus“ uváděný v návrhu zahrnuje situace, kdy fyzická nebo právnická osoba zpřístupňuje data dobrovolně pro opakované použití, bez protiplnění, pro *„ cíle obecného zájmu, jako jsou účely vědeckého výzkumu či zlepšení veřejných služeb“*[74].

158. Lze tvrdit, že návrh „nevytváří“, ale „formalizuje/kodifikuje“ možnost držitelů dat (mezi něž podle návrhu patří i subjekty údajů) dobrovolně zpřístupnit data, což již předpokládá nařízení GDPR. Subjekt údajů již má možnost souhlasit se zpracováním osobních údajů, které se ho týkají, mimo jiné pro účely vědeckého výzkumu.

159. Navzdory definici podle čl. 2 odst. 10 návrhu („‚datovým altruismem‘ [se rozumí] souhlas udělený subjekty údajů ke zpracovávání osobních údajů, které se jich týkají, nebo svolení jiných držitelů dat, jež umožňuje použití jejich neosobních údajů, aniž by se vyžadovala odměna, pro cíle obecného zájmu, jako jsou účely vědeckého výzkumu či zlepšení veřejných služeb“) není pojem „*datový altruismus*“ stále ještě jasně a dostatečně definován. Zejména není jasné, zda souhlas předpokládaný v návrhu odpovídá pojmu „souhlas“ podle GDPR, včetně podmínek zákonnosti takového souhlasu. Není navíc ani jasné, jakou přidanou hodnotu „datový altruismus“ má, vezmeme-li v úvahu již existující právní rámec pro souhlas podle GDPR, který stanoví konkrétní podmínky platnosti souhlasu.

160. GDPR a návrh se v případě zpracování osobních údajů organizacemi pro datový altruismus uplatňují současně. EDPB a EIOÚ podporují cíl usnadnit zpracování osobních údajů pro přesně definované účely obecného zájmu, nicméně tohoto cíle má být dosaženo v plném souladu s příslušnými pravidly a zásadami ochrany údajů. EDPB a EIOÚ zejména zdůrazňují, že jedním z hlavních cílů nařízení GDPR je zajistit, aby si subjekt údajů ponechal kontrolu nad svými osobními údaji. V této souvislosti EDPB a EIOÚ zdůrazňují, že **je třeba splnit všechny požadavky týkající se souhlasu stanovené v GDPR**.

161. EDPB a EIOÚ znovu opakují, že **základního práva na ochranu osobních údajů se dotyčná fyzická osoba v žádném případě nemůže „vzdát“**, byť jde o „akt altruismu“ související s osobními údaji. Správce údajů (organizace pro datový altruismus) zůstává plně vázán pravidly a zásadami v oblasti osobních údajů, i když subjekt údajů udělil organizaci pro datový altruismus souhlas se zpracováním osobních údajů, které se ho týkají, pro jeden nebo více stanovených účelů.

162. **S ohledem na výše uvedené by návrh měl ve věcné části upřesnit, že odkazuje na souhlas ve smyslu čl. 4 odst. 11 GDPR a že podle čl. 7 odst. 3 organizace pro datový altruismus zajistí, aby odvolání souhlasu bylo stejně snadné jako jeho poskytnutí[75].**

---

[74] Ustanovení čl. 2 odst. 10 návrhu.

[75] Viz Pokyny EDPB 5/2020 k souhlasu, body 121–122:
„121. Článek 6 stanoví podmínky pro zákonné zpracování osobních údajů a popisuje šest právních základů, které správce může využít. Uplatnění jednoho z těchto šesti základů musí být stanoveno před činností zpracování a ve vztahu ke konkrétnímu účelu.

163. EDPB a EIOÚ rovněž zdůrazňují skutečnost, že data zpracovávaná organizacemi pro datový altruismus mohou zahrnovat zvláštní kategorie osobních údajů, např. údaje týkající se zdraví.

164. EDPB a EIOÚ rovněž podtrhují, že v souladu se zásadou minimalizace údajů, je-li to možné a přiměřené účelu, by data měla být zpracovávána v anonymizované podobě.

165. EDPB a EIOÚ vítají, že návrh podle čl. 22 odst. 3 určuje, že jsou-li osobní údaje poskytovány organizaci pro datový altruismus, formulář souhlasu v souladu s GDPR zajistí, aby fyzické osoby byly schopny poskytnout a odvolat souhlas pro konkrétní operaci zpracování údajů.

166. V této souvislosti se EDPB a EIOÚ domnívají, že pravidla pro odvolání souhlasu, včetně jeho důsledků, by měla být jasná. Mělo by být zejména jasné, jakým způsobem organizace pro datový altruismus i uživatelé dat vyhovují žádostem o odvolání, mimo jiné vymazáním osobních údajů v souladu s čl. 17 odst. 1 písm. b) GDPR. EDPB a EIOÚ připomínají, že při rozhodování o „datovém altruismu“ může být nutné, aby organizace pro datový altruismus provedly v souladu s článkem 35 GDPR posouzení vlivu na ochranu osobních údajů.

167. Vědecký výzkum často zahrnuje zpracování a sdílení zvláštních kategorií osobních údajů ve velkém měřítku, a toto sdílení by tudíž v některých případech mohlo být podle GDPR považováno za vysoce rizikové zpracování údajů. Posouzení vlivu na ochranu osobních údajů by navíc měla být v této souvislosti prováděna za účasti pověřence pro ochranu osobních údajů a etického kontrolního výboru, a tato posouzení nebo případně jejich shrnutí by měla být zveřejněna v rámci dobré praxe, a pokud to bude možné.

168. Podle GDPR by souhlas měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení.

169. Ve 33. bodě odůvodnění GDPR je zdůrazněno, že často není možné v době shromažďování osobních údajů v plném rozsahu stanovit účel zpracování osobních údajů pro účely vědeckého výzkumu. Subjektům údajů by proto mělo být umožněno, aby udělily svůj souhlas ohledně určitých oblastí vědeckého výzkumu v souladu s uznávanými etickými normami pro vědecký výzkum[76]. To se odrazilo i ve 38. bodu odůvodnění návrhu.

170. EDPB a EIOÚ však zdůrazňují, že udělení tohoto druhu souhlasu pro účely obecného zájmu[77] jako takového (nedefinovaného přesně a odkazujícího na jiný a mnohem širší rozsah než vědecký výzkum) není podle GDPR povoleno.

---

122. Je důležité si zde povšimnout, že **pokud se správce pro kteroukoli část zpracování rozhodne použít souhlas, musí být připraven respektovat toto své rozhodnutí a zastavit tuto část zpracování, pokud jednotlivec souhlas odvolá.** Tvrdit, že údaje budou zpracovány na základě souhlasu, a přitom se ve skutečnosti opírat o jiný právní základ, by bylo k fyzickým osobám zásadně nekalé.“

[76] Viz nedávno přijaté Pokyny EDPB k souhlasu, pokyny 5/2020, zejména k souhlasu pro účely vědeckého výzkumu na stranách 30–32.

[77] Viz Pokyny EDPB 3/2020 ke zpracování údajů o zdravotním stavu pro účely vědeckého výzkumu v souvislosti s rozšířením onemocnění COVID-19, body 42–45:

171. Návrh ve svém 35. bodě odůvodnění ve skutečnosti odkazuje na „cíle veřejného zájmu“ tím, že poskytuje (nikoli definici, ale) nevyčerpávající seznam příkladů, který zahrnuje aplikovaný a ze soukromých prostředků financovaný výzkum a technologický rozvoj a analýzu dat[78].

172. **S ohledem na výše uvedené se EDPB a EIOÚ domnívají, že by Komise měla lépe definovat cíle obecného zájmu takovéhoto „datového altruismu“. EDPB a EIOÚ se domnívají, že tato nedostatečná definice může vést k právní nejistotě, jakož i ke snížení úrovně ochrany osobních údajů v EU. Například požadavek, aby organizace pro datový altruismus informovala držitele dat (včetně subjektu údajů) „o cílech obecného zájmu, pro něž povoluje zpracovávání jejich údajů uživatelem dat“, je v souladu se zásadou, podle níž se budou data shromažďovat pro určité, výslovně vyjádřené a legitimní cíle a nebudou dále zpracovávány způsobem, který je s těmito cíli neslučitelný (zásada účelového omezení podle čl. 5 písm. b) GDPR. Návrh by proto měl obsahovat vyčerpávající seznam jasně vymezených cílů.** EPDB a EIOÚ si zároveň všímají upřesnění uvedeného ve 38. bodě odůvodnění návrhu[79]. Toto upřesnění bude zahrnuto do věcné části návrhu, nejen do bodu odůvodnění, a bude v návrhu doplněno jasným rozlišením mezi:

„42. Obecně musí být údaje podle čl. 5 odst. 1 písm. b) GDPR „shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný“.
43. Avšak „domněnka slučitelnosti“ obsažená v čl. 5 odst. 1 písm. b) GDPR stanoví, že „další zpracování […] pro **účely vědeckého** […] **výzkumu** […] se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely“. Tomuto tématu se vzhledem k jeho horizontální a komplexní povaze budou podrobněji věnovat plánované **pokyny EDPB ke zpracování údajů o zdravotním stavu pro účely vědeckého výzkumu**.
44. Čl. 89 odst. 1 nařízení GDPR stanoví, že zpracování údajů pro účely výzkumu „podléhá […] **vhodným zárukám**“ a že tyto „záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace údajů. Tato opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely“.
45. Požadavky čl. 89 odst. 1 GDPR zdůrazňují význam zásady minimalizace údajů a zásady integrity a důvěrnosti, jakož i zásady záměrné a standardní ochrany osobních údajů (viz níže). Vzhledem k citlivé povaze údajů o zdravotním stavu a rizikům při opakovaném použití údajů o zdravotním stavu pro účely vědeckého výzkumu tak musí být přijata přísná opatření, aby byla zajištěna vhodná úroveň bezpečnosti, jak je požadováno podle čl. 32 odst. 1 GDPR.“
Viz rovněž dokument EDPB v reakci na žádost Evropské komise o vyjasnění důsledného uplatňování GDPR se zaměřením na zdravotní výzkum, přijatý dne 2. února 2021.

[78] Ustanovení 35. bodu odůvodnění: „K těmto cílům by patřila zdravotní péče, boj proti změně klimatu, zlepšení mobility, snazší tvorba oficiálních statistik nebo lepší poskytování veřejných služeb. Za cíle veřejného zájmu by se měla pokládat rovněž podpora vědeckého výzkumu, včetně například technologického rozvoje a demonstrací, základního výzkumu, aplikovaného výzkumu a výzkumu financovaného ze soukromých zdrojů. Toto nařízení má přispět ke vzniku datových souborů zpřístupněných na základě datového altruismu, které jsou dostatečně velké na to, aby umožnily analýzy dat a strojové učení, a to i napříč hranicemi v Unii.“

[79] 38. bod odůvodnění: „‚Organizace pro datový altruismus uznané v Unii‘ **by měly mít možnost shromažďovat příslušná data přímo od fyzických a právnických osob nebo zpracovávat údaje shromážděné jinými subjekty**. **Datový altruismus by se obvykle zakládal na souhlasu** subjektů údajů ve smyslu čl. 6 odst. 1 písm. a) a čl. 9 odst. 2 písm. a) a byl v souladu s požadavky na právoplatný souhlas podle článku 7 nařízení (EU) 2016/679.
Podle nařízení (EU) 2016/679 lze **účely vědeckého výzkumu** podpořit souhlasem **s určitými oblastmi vědeckého výzkumu** v souladu s uznávanými etickými normami pro vědecký výzkum nebo pouze s určitými oblastmi výzkumu nebo částmi výzkumných projektů.
V čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679 je stanoveno, že by se **další zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely** nemělo v souladu s čl. 89 odst. 1 nařízení (EU) 2016/679 považovat za neslučitelné s původními účely.“

– souhlasem pro oblasti vědeckého souhlasu,

– dalším zpracováním pro účely vědeckého nebo historického výzkumu nebo pro statistické účely a

– zpracováním pro cíle obecného zájmu (má být definováno v návrhu).

173. EDPB a EIOÚ navíc konstatují, že je třeba objasnit pojem „datová úložiště“ ve 36. bodě odůvodnění[80], uvedený pouze v tomto bodě odůvodnění, a nikoli ve věcné části návrhu, který souvisí se zpracováním osobních i neosobních údajů.

3.5.2 Články 16 a 17: režim registrace – obecné požadavky na způsobilost k registraci – obsah registrace; výsledek (a načasování) registrace

174. Kapitola IV návrhu zavádí pro organizace zapojené do „datového altruismu“ možnost registrovat se jako „organizace pro datový altruismus uznaná v Unii“[81] s deklarovaným cílem zvýšit důvěru občanů v činnost těchto organizací. V této souvislosti EDPB a EIOÚ zdůrazňují, že návrh neobjasňuje, zda je registrace povinná či nikoli, ani to, zda se ustanovení kapitoly IV použijí také v případě, že organizace pro datový altruismus nejsou registrovány.

175. Obecné požadavky na registraci jsou uvedeny v článku 16; požadavky na registraci jsou stanoveny v článku 17 a zejména v čl. 17 odst. 4 písm. a) až i). „Prověřování“ organizace pro datový altruismus se omezuje na ověření požadavků podle článku 16 a čl. 17 odst. 4 příslušným orgánem a proběhne do dvanácti týdnů ode dne podání žádosti. Návrh však nedefinuje druh ověření, které má příslušný orgán za úkol.

176. V této souvislosti EDPB a EIOÚ poznamenávají, že k zajištění náležitých kontrol a v konečném důsledku ke zvýšení důvěry by byl vhodnější režim poskytující silnější záruky v případě zpracování osobních údajů než „lehčí“ režim registrace (v podstatě jednoduše „deklaratorní“ režim) stanovený v návrhu a podobný režimu předpokládanému pro poskytovatele služeb sdílení dat.

177. EDPB a EIOÚ zdůrazňují, že skutečnost, že z právního, technického a organizačního hlediska nejsou na vytvoření „organizace pro datový altruismus uznané v Unii“ (nebo „poskytovatele sdílení dat“) kladeny téměř žádné požadavky, je problematická. Například organizace, která je podle čl. 15 odst. 3 návrhu oprávněna se „ve své písemné a ústní komunikaci označovat za ‚organizaci pro datový altruismus uznanou v Unii‘ (‚účinek označování‘), bude s největší pravděpodobností shromažďovat osobní údaje s využitím očekávání občanů, zejména pokud jde o plné dodržování ochrany údajů stejnou organizací.

178. EDPB a EIOÚ zdůrazňují, že organizace pro datový altruismus musí být důvěryhodné subjekty. Pokud jde o obecné požadavky na registraci (stanovené v článku 16 návrhu), EDPB a EIOÚ se rovněž

[80] 36. bod odůvodnění: „Právní subjekty, které usilují o podporu cílů **obecného zájmu** rozsáhlým zpřístupňováním příslušných dat na základě datového altruismu a splňují určité požadavky, by měly mít možnost registrovat se jako ‚Organizace pro datový altruismus uznané v Unii‘. To by mohlo vést k vytváření **datových úložišť**.[…]“

[81] Ustanovení 36. bodu odůvodnění návrhu.

domnívají, že by měla být vyjasněna nezávislost organizace pro datový altruismus (např. právní, organizační, ekonomická) na ziskových subjektech předpokládaná v čl. 16 písm. b) návrhu[82].

179. **EDPB a EIOÚ zejména doporučují zavést přímý odkaz na požadavky na ochranu údajů v článku 16, především na technické a organizační požadavky umožňující uplatňování norem ochrany údajů a výkon práv subjektů údajů.**

180. **S ohledem na výše uvedené prvky a vzhledem k možným dopadům na subjekty údajů při zpracování osobních údajů, které může provést organizace pro datový altruismus, se EDPB a EIOÚ domnívají, že režim registrace podle návrhu nestanoví dostatečně přísný postup prověřování vztahující se na takovouto organizaci. EDPB a EIOÚ doporučují prozkoumat alternativní postupy, které by zejména měly zohlednit systematičtější zahrnutí nástrojů odpovědnosti a dodržování předpisů pro zpracování osobních údajů podle GDPR, především dodržování kodexu chování nebo mechanismu pro vydávání osvědčení.**

3.5.3 Články 18 a 19: požadavky na transparentnost a „[z]vláštní požadavky na ochranu práv a zájmů subjektů údajů a právních subjektů s ohledem na jejich údaje“

181. EDPB a EIOÚ konstatují, že požadavky doprovázející režim registrace by měly posílit, **nikoli však nahradit povinnosti organizací pro datový altruismus jako správců nebo zpracovatelů podle GDPR**.

182. EDPB a EIOÚ konstatují, že 36. bod odůvodnění návrhu je v této souvislosti nejasný, jelikož zdánlivě znamená, že prostředky k odvolání souhlasu poskytne organizace pro datový altruismus jednající jako zpracovatel[83]. Kvalifikace organizace pro datový altruismus jako zpracovatele namísto správce však vyžaduje další posouzení, protože se v kontextu návrhu nezdá být jediným možným scénářem.

183. Rovněž by měl být jasně vymezen podpůrný účinek registrace (jako organizace pro datový altruismus), zejména s ohledem na aspekt právního základu pro zpracování osobních údajů podle GDPR[84]. V této souvislosti EDPB a EIOÚ znovu opakují, že **režim registrace nemůže** v zájmu zákonnosti zpracování

---

[82] „Aby byla organizace pro datový altruismus způsobilá pro registraci, musí: […] b) působit na neziskovém základě a **být nezávislá na jakémkoli subjektu, který usiluje o zisk**“ (zvýraznění doplněno);

[83] 36. bod odůvodnění stanoví (zvýraznění doplněno): „**Další záruky** by měly zahrnovat možnost **zpracovávat příslušná data v bezpečném zpracovatelském prostředí** provozovaném registrovaným subjektem, **mechanismy dozoru**, jako jsou rady nebo výbory pro etiku, aby bylo zajištěno, že správce údajů dodržuje vysoké standardy vědecké etiky, **účinné technické prostředky pro možnost souhlas** kdykoli odvolat nebo změnit, a to **na základě informačních povinností zpracovatelů údajů podle nařízení (EU) 2016/679**, jakož i **prostředky umožňující informovat subjekty údajů** o použití údajů, které zpřístupní.“ (zvýraznění doplněno)

[84] V této souvislosti 38. bod odůvodnění návrhu stanoví toto (zvýraznění doplněno): „‚Organizace pro datový altruismus uznané v Unii‘ **by měly mít možnost shromažďovat příslušná data přímo od fyzických a právnických osob** nebo zpracovávat údaje shromážděné jinými subjekty. Datový altruismus by se **obvykle** zakládal na souhlasu subjektů údajů ve smyslu čl. 6 odst. 1 písm. a) a čl. 9 odst. 2 písm. a) a byl v souladu s požadavky na právoplatný souhlas podle článku 7 nařízení (EU) 2016/679. Podle nařízení (EU) 2016/679 lze účely vědeckého výzkumu podpořit souhlasem s určitými oblastmi vědeckého výzkumu v souladu s uznávanými etickými normami pro vědecký výzkum nebo pouze s určitými oblastmi výzkumu nebo částmi výzkumných projektů. V čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679 je stanoveno, že by se další zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely nemělo v souladu s čl. 89 odst. 1 nařízení (EU) 2016/679 považovat za neslučitelné s původními účely.“

údajů **nahradit nezbytnost vhodného právního důvodu pro zpracování osobních údajů podle čl. 6 odst. 1 GDPR**. Jinými slovy, podle GDPR je zpracování zákonné, pouze pokud se uplatňuje nejméně jeden z právních základů podle čl. 6 odst. 1 GDPR a pouze v odpovídajícím rozsahu.

184. S ohledem na článek 18 návrhu mají EDPB a EIOÚ pochybnosti o tom, jak je zachována nezávislost organizace pro datový altruismus v případech, kdy je její financování založeno na *„případných poplat[cích] hrazených fyzickými nebo právnickými osobami zpracovávajícími údaje“* [85] (tj. údaje poskytované těmto fyzickým nebo právnickým osobám organizací pro datový altruismus). EDPB a EIOÚ se dále domnívají, že návrh by měl lépe vysvětlit, v jakých situacích může organizace pro datový altruismus účtovat poplatky fyzickým nebo právnickým osobám za zpracování údajů „svěřených“ subjekty údajů pro „datový altruismus“.

185. I v tomto případě, jak bylo poznamenáno ohledně opakovaného použití dat v držení subjektů veřejného sektoru, existuje otázka související s pobídkami pro správce, aby vybízel k většímu zpracování osobních údajů, v tomto případě k většímu „datovému altruismu“. Kvalifikace organizací pro datový altruismus jako registrovaných subjektů, které mají neziskový charakter (36. bod odůvodnění), což EDPB a EIOÚ vítají, zmíněnou otázku zmírňuje pouze částečně.

186. Znění 36. bodu odůvodnění, které zmiňuje požadavky na organizace pro datový altruismus, vzbuzuje obavy, protože odkazuje na „dobrovolné dodržování“, rovněž s ohledem na otázky týkající se (povinného) souladu s GDPR[86].

187. Uvedený bod odůvodnění je rovněž v rozporu (pokud není zdůrazněna volitelná povaha požadavků podle 36. bodu odůvodnění) s věcnou částí návrhu, čl. 17 odst. 3, který zmiňuje organizace pro datový altruismus, jež nejsou usazeny v Unii.

188. **Pokud jde o článek 19 návrhu, EDPB a EIOÚ jsou toho názoru, že by měl být doplněn výslovný odkaz na články 13 a 14 GDPR, aby byl zajištěn soulad mezi tímto článkem návrhu a povinnostmi týkajícími se zásady transparentnosti podle GDPR, a aby organizace pro datový altruismus a uživatelé dat poskytovaly subjektu údajů potřebné informace o zpracování osobních údajů, které se ho týkají**.

189. Podle EDPB a EIOÚ se navíc zdá, že současné znění čl. 19 odst. 1 písm. a)[87] je nejasné a že je obtížné jej sladit s ustanoveními GDPR.

---

[85] Viz čl. 18 odst. 1 písm. d) návrhu.

[86] Ustanovení 36. bodu odůvodnění (zvýraznění doplněno): „[…] **Dobrovolné dodržování určitého souboru požadavků** těmito registrovanými subjekty by mělo zajistit důvěru v to, že data zpřístupněná pro altruistické účely slouží cíli obecného zájmu. Tato **důvěra** by měla plynout zejména ze **sídla v Unii**, jakož i z požadavku, aby registrované subjekty měly **neziskový charakter**, z požadavků na **transparentnost** a ze **zvláštních záruk** zavedených na ochranu práv a zájmů **subjektů údajů a společností**. **Další záruky** by měly zahrnovat možnost zpracovávat příslušná data v **bezpečném zpracovatelském prostředí** provozovaném registrovaným subjektem, **mechanismy dozoru**, jako jsou rady nebo výbory pro etiku, aby bylo zajištěno, že správce údajů dodržuje vysoké standardy vědecké etiky, účinné **technické prostředky pro možnost souhlas** kdykoli odvolat nebo změnit, a to na základě informačních povinností zpracovatelů údajů podle nařízení (EU) 2016/679, jakož i prostředky umožňující **informovat** subjekty údajů o použití údajů, které zpřístupní.“

[87] Ustanovení čl. 19 odst. 1 písm. a) uvádí (zvýraznění doplněno): „Každý subjekt zapsaný v rejstříku uznaných organizací pro datový altruismus informuje držitele dat: a) **o cílech obecného zájmu, pro něž povoluje zpracovávání jejich údajů uživatelem dat**, a to snadno srozumitelným způsobem.“

190. **Pokud jde o tuto kapitolu návrhu, měl by v zájmu ochrany dotčených osob před nepřiměřenými riziky pro jejich základní práva a svobody zvláštní význam také výslovný důraz na poskytování anonymizovaných údajů, pokud je to možné a přiměřené účelu zpracování údajů v souladu se zásadou minimalizace údajů, zejména v případě zpracování zvláštních kategorií údajů.**

3.5.4 Články 20 a 21: orgány příslušné pro registraci a sledování souladu

191. **Pokud jde o čl. 20 odst. 3 návrhu, EDPB a EIOÚ se domnívají, že je třeba posílit správu a sledování souladu, aby bylo zajištěno vhodnější prověřování organizací pro datový altruismus včetně souladu s GDPR a jasné vymezení dohledu nad ustanoveními návrhu způsobem, který stanoví, že v případě záležitosti týkající se osobních údajů budou plně dodržovány požadavky na ochranu údajů a že zůstanou v příslušnosti úřadů pro ochranu údajů zřízených podle GDPR.**

192. **Určení úřadů pro ochranu údajů jako hlavních příslušných orgánů pro dohled nad ustanoveními kapitoly IV návrhu a jejich vymáhání by rovněž zajistilo jednotnější regulační přístup napříč členským státem a přispělo by tak k důslednému uplatňování návrhu. Pokud jde o jejich příslušnost a úkoly podle GDPR, mají úřady pro ochranu údajů již specifické odborné znalosti v oblasti sledování souladu zpracování údajů, auditu konkrétních činností zpracování údajů a sdílení dat, posouzení vhodných opatření k zajištění vysoké míry bezpečnosti uchovávání a přenosu osobních údajů, jakož i v oblasti zvyšování povědomí správců a zpracovatelů o jejich povinnosti související se zpracováním osobních údajů.**

193. EDPB a EIOÚ se navíc domnívají, že při sledování souladu nelze pravomoc příslušných orgánů omezit na „oprávnění vyžádat si informace“, jak vyplývá z čl. 21 odst. 2 návrhu. Toto omezení rozhodně pramení z deklaratorní povahy „režimu označování“ předpokládaného návrhem, i když neodpovídá úrovni prověřování, kterou označování vyžaduje, a to vzhledem k vysokým očekáváním souladu ochrany údajů vyplývajícím z takového označování, zejména vůči subjektům údajů.

194. EDPB a EIOÚ zdůrazňují, že úřadům pro ochranu údajů by měly být poskytnuty odpovídající zdroje, aby mohly účinně a efektivně vykonávat nezbytný dohled. EDPB a EIOÚ dále v této souvislosti konstatují, že 28. bod odůvodnění, který odkazuje na poskytovatele služeb sdílení dat, uvádí, že *„[t]ímto nařízením by neměla být dotčena povinnost poskytovatelů služeb sdílení dat dodržovat nařízení (EU) 2016/679 a odpovědnost dozorových úřadů za zajištění souladu s tímto nařízením“*. Stejný požadavek by měl být uveden v souvislosti s organizacemi pro datový altruismus.

3.5.5 Článek 22: evropský formulář souhlasu s datovým altruismem

195. Článek 22 návrhu zmocňuje Komisi, aby pomocí prováděcích aktů přijala „evropský formulář souhlasu s datovým altruismem“[88]. V této souvislosti článek 22, jak je upřesněno ve 41. bodě odůvodnění, stanoví, že formulář souhlasu má být zaveden prostřednictvím prováděcího aktu Komise za pomoci Evropského sboru pro datové inovace, a to po konzultaci s EDPB.

[88] Ustanovení čl. 22 odst. 1: „Aby se usnadnil sběr údajů na základě datového altruismu, může Komise přijmout prováděcí akty za účelem vypracování evropského formuláře souhlasu s datovým altruismem. Formulář umožní získávání souhlasu ve všech členských státech v jednotné podobě. Tyto prováděcí akty se přijímají poradním postupem podle čl. 29 odst. 2.“

196. **V této souvislosti se EDPB a EIOÚ domnívají, že návrh by měl zavést závaznější, lépe strukturovaný a institucionalizovaný mechanismus než pouhou konzultaci s EDPB.**

3.6 Mezinárodní předávání dat: čl. 5 odst. 9 až 13; 17. a 19. bod odůvodnění; článek 30

197. I když se ustanovení návrhu týkající se předávání dat do třetích zemí zdají *a priori* omezena pouze na neosobní údaje, je pravděpodobné, že během jejich uplatňování vyvstanou otázky právního a politického souladu s právním rámcem EU pro ochranu údajů, zejména pokud jsou osobní a neosobní údaje souboru dat neoddělitelně propojeny.

198. Přestože se zdá, že záměrem Komise je osobní údaje vyloučit, omezení rozsahu ustanovení o předávání dat na neosobní údaje není v návrhu pokaždé jasně zohledněno. Na osobní údaje, pokud jsou zároveň důvěrnými údaji nebo daty chráněnými právy duševního vlastnictví, by se mohla vztahovat zejména ustanovení čl. 5 odst. 9 a čl. 5 odst. 10 týkající se předávání dat v držení subjektů veřejného sektoru[89].

199. **Návrh současně obsahuje ustanovení (čl. 5 odst. 11), které by mohlo být považováno za více „ochranné" pro neosobní údaje než pro osobní údaje, jelikož podle návrhu by Komise mohla v konečném důsledku přijmout prostřednictvím aktu v přenesené pravomoci[90] zvláštní podmínky pro předávání neosobních údajů do některých třetích zemí, jejichž nesplnění může vést až k zákazu předávání[91].**

200. **Možnost, aby Komise prostřednictvím prováděcího aktu [92] přijala „rozhodnutí o odpovídající ochraně" pro předávání neosobních údajů do dané třetí země, by také pravděpodobně vyvolala otázky interakce a souladu s nástroji pro předávání stanovenými v GDPR pro předávání osobních údajů do téže třetí země.**

201. **V každém případě je v zájmu zajištění souladu s právním rámcem pro ochranu údajů důležité v této souvislosti připomenout, že v případě „smíšených datových souborů" se použije GDPR, zejména jeho kapitola V.**

202. EDPB a EIOÚ konstatují, že článek 30 návrhu[93] zmiňuje pouze neosobní údaje, a zdá se, že jeho odstavec 2 odráží ustanovení článku 48 nařízení GDPR (s tím rozdílem, že čl. 30 odst. 2 zavádí v souvislosti s dotčenými mezinárodními dohodami časové omezení).

203. Podle čl. 30 odst. 3 návrhu subjekty (subjekt veřejného sektoru, subjekt, kterému bylo povoleno opakované použití, poskytovatel služeb sdílení dat, organizace pro datový altruismus), které obdrží rozhodnutí soudu nebo správního orgánu třetí země, které jim ukládá předat neosobní údaje z Unie či umožnit přístup k neosobním údajům v Unii, si podle návrhu vyžádají stanovisko příslušných orgánů

---

[89] Viz čl. 5 odst. 10 návrhu: „Subjekty veřejného sektoru předají důvěrné údaje nebo data chráněná právy duševního vlastnictví dalšímu uživateli, který má v úmyslu předat data do jiné třetí země, než je země určená v souladu s odstavcem 9, pouze tehdy, pokud se další uživatel zaváže: a) dodržovat povinnosti uložené podle odstavců 7 až 8 i po předání dat do třetí země a b) uznat pravomoc soudů členského státu subjektu veřejného sektoru, pokud jde o spory týkající se plnění povinnosti uvedené v písmenu a)."

[90] Viz 19. bod odůvodnění návrhu.

[91] Viz 19. bod odůvodnění návrhu.

[92] Viz čl. 5 odst. 9 až 11 návrhu.

[93] Článek 30 Mezinárodní přístup, zahrnutý do kapitoly VIII Závěrečná ustanovení.

nebo subjektů podle návrhu za účelem zjištění, zda jsou použitelné podmínky předání splněny (čl. 30 odst. 3 poslední věta).

204. Konzultace s příslušným orgánem je nezbytná, pokud by v případě rozhodnutí soudu nebo správního orgánu třetí země „hrozilo, že by příjemce jednal v rozporu s unijními právními předpisy nebo s právními předpisy příslušného členského státu“ (čl. 30 odst. 3)[94].

205. Zdá se, že toto ustanovení ve srovnání s článkem 48 GDPR jde o krok dál tím, že v konkrétních případech vyžaduje konzultaci s příslušným orgánem. V této souvislosti by tedy mohlo být nějakým způsobem považováno za více „ochranné“ pro neosobní údaje než pro osobní údaje, jelikož takové oznámení GDPR nepředpokládá.

3.7 Horizontální ustanovení o institucionálním prostředí; stížnosti; odborná skupina Evropského sboru pro datové inovace; akty v přenesené pravomoci; sankce, hodnocení a přezkum, změny nařízení o jednotné digitální bráně, přechodná opatření a vstup v platnost

3.7.1 Článek 23: požadavky týkající se příslušných orgánů

206. Kapitola V návrhu stanoví požadavky na fungování příslušných orgánů určených ke sledování a uplatňování rámce pro oznamování pro poskytovatele služeb sdílení dat a subjekty zapojené do datového altruismu. Z kapitol III a IV návrhu plyne, že tyto příslušné orgány se liší od úřadů pro ochranu údajů. Ve skutečnosti požadavky zavedené v článku 23 návrhu naznačují „technický“ charakter těchto orgánů, *„jsou právně odlišeny a funkčně nezávislé na všech poskytovatelích služeb sdílení dat či subjektech uvedených v rejstříku uznaných organizací pro datový altruismus“.*

207. V této souvislosti se úloha dozorových úřadů pro ochranu údajů jeví jako omezená – podle kapitoly III – na pouhou výměnu informací s příslušným orgánem a – podle kapitoly IV – na spolupráci s tímto orgánem a poskytnutí stanoviska nebo rozhodnutí týkajících se otázek vyžadujících posouzení souladu s GDPR na žádost příslušného orgánu. Návrh kromě toho nedefinuje, jak a do jaké míry budou úřady pro ochranu údajů komunikovat s takovými příslušnými orgány, ani to, jaké finanční a lidské zdroje

[94] Výše uvedené podmínky v čl. 30 odst. 3 zřejmě stačí k **nahrazení podmínek uvedených v odstavci 2, a nahrazují tak mezinárodní pravidla uvedená v tomto odstavci**. V čl. 30 odst. 4 je stanoveno: „Nejsou-li podmínky uvedené v odstavci 2 **nebo odstavci 3** splněny, **subjekt veřejného sektoru, fyzická nebo právnická osoba, jíž bylo uděleno právo na opakované použití dat podle Kapitoly 2, poskytovatel služeb sdílení dat nebo případně subjekt zapsaný v rejstříku uznaných organizací pro datový altruismus poskytne v reakci na žádost minimální povolené množství dat**, a to na základě přiměřeného výkladu žádosti.“ (zvýraznění doplněno)
Tato ustanovení návrhu by mohla být **v rozporu s jinými právními předpisy Unie nebo členského státu, zejména pokud jde o justiční spolupráci v trestních nebo občanských věcech**. Význam této připomínky podle právních předpisů o ochraně údajů je dán skutečností, že **v případě nesprávného výkladu pojmu neosobní údaje existuje vysoké riziko, že subjekty veřejného sektoru, poskytovatelé služeb sdílení dat, organizace pro datový altruismus, další uživatelé dat a uživatelé dat předají osobní údaje do třetí země s (výrazně) nižším standardem ochrany dotčených osob**.

jsou předpokládány, aby úřadům pro ochranu údajů umožnily vykonávat úkoly vyžadované takovou interakcí.

208. EDPB a EIOÚ konstatují, že mnoho ustanovení návrhu, nad nimiž vykonávají dohled pověřené příslušné orgány určené podle článků 12 a 20, souvisí s ochranou osobních údajů. S ohledem na tuto skutečnost **EDPB a EIOÚ zdůrazňují, že příslušnost a pravomoci nezávislých dozorových úřadů musí být plně respektovány, jelikož jim je svěřena odpovědnost za ochranu základních práv a svobod fyzických osob v souvislosti se zpracováním a za usnadnění volného toku osobních údajů, jak je stanoveno v nařízeních GDPR a EUDPR, v souladu s článkem 16 SFEU a článkem 8 Listiny a v souladu s příslušnou judikaturou Soudního dvora Evropské unie[95]. Vzhledem k výše uvedenému EDPB a EIOÚ doporučují, aby návrh výslovně uznal, že pokud jde o osobní údaje, jsou úřady pro ochranu údajů hlavními příslušnými orgány ke sledování souladu s ustanoveními kapitol III a IV návrhu, v případě potřeby po konzultaci s dalšími příslušnými odvětvovými orgány. Jak již bylo zdůrazněno, těmto orgánům by měly být poskytnuty vhodné zdroje, které jim umožní účinně a efektivně vykonávat nezbytný dohled.**

3.7.2 Článek 24: stížnosti; článek 25: právo na účinnou soudní ochranu

209. EDPB a EIOÚ konstatují, že článek 24 stanoví, že *„[f]yzické a právnické osoby mají právo podat dotčenému příslušnému vnitrostátnímu orgánu stížnost na poskytovatele služeb sdílení dat nebo na subjekt zapsaný v rejstříku uznaných organizací pro datový altruismus“*, neupřesňuje však možný obsah stížnosti (konkrétně na jaké porušení návrhu). Rovněž se zdá, že stížnosti na subjekty veřejného sektoru nebo další uživatele uvedené v kapitole II návrhu nejsou možné a v článku 24 návrhu nejsou předpokládány.

210. Článek 25 navíc stanoví právo na účinnou soudní ochranu jakékoli dotčené fyzické nebo právnické osoby, pokud jde o nečinnost při řešení stížnosti podané u příslušného orgánu, jakož i o rozhodnutí příslušných orgánů uvedených v článcích 13, 17 a 21 (rozhodnutí týkající se dohledu nad službami sdílení dat, registrace organizací pro datový altruismus, resp. sledování souladu registrovaných organizací pro datový altruismus).

211. EDPB a EIOÚ podotýkají, že výše uvedená ustanovení návrhu týkající se práva podat stížnost u relevantního vnitrostátního příslušného orgánu (článek 24) a práva na účinný soudní prostředek nápravy proti nečinnosti nebo rozhodnutím výše uvedeného příslušného orgánu (článek 25) by mohla zvýšit riziko souběžných a odporujících si režimů mezi GDPR a návrhem, zdůrazněné v tomto stanovisku. Například stížnosti týkající se služeb zprostředkování, které pro subjekty údajů zajišťují dostupnost prostředků k výkonu práv stanovených v GDPR (viz čl. 9 odst. 1 písm. b)), by podle návrhu spadaly do působnosti příslušných orgánů. Jinými slovy, nesoulad a přesahy „hmotného práva“ by také „eskalovaly“ do přesahů příslušnosti ve správních a soudních řízeních.

---

[95] Viz mimo jiné rozsudek ESD ze dne 9. března 2010, *Evropská komise v. Spolková republika Německo*, ve věci C-518/07, k dispozici na adrese: https://curia.europa.eu/juris/liste.jsf?language=cs&num=C-518/07.
Ve svém rozsudku ze dne 9. března 2010 Soudní dvůr konstatoval, že na úřady pro ochranu údajů by měly být uchráněny od jakéhokoli přímého či nepřímého vnějšího vlivu. K vyvození závěru, že úřad pro ochranu údajů nemůže jednat zcela nezávisle, stačí pouhé riziko vnějšího vlivu.

212. Z tohoto důvodu **EDPB a EIOÚ požadují jasnou, jednoznačnou a velmi přesnou definici hmotněprávních pravidel návrhu, nad nimiž vykonávají dohled pověřené příslušné orgány**, **a jeho mechanismu sledování, který zajišťuje plný soulad s GDPR**.

3.7.3 Články 26 a 27: složení a úkoly odborné skupiny Evropského sboru pro datové inovace

213. Kapitola VI návrhu *„zřizuje formální odbornou skupinu („Evropský sbor pro datové inovace"), která usnadní vytváření osvědčených postupů orgány členských států, zejména při vyřizování žádostí o opakované použití dat, na něž se vztahují práva jiných osob (podle kapitoly II), při zajišťování ustálené praxe, pokud jde o rámec pro oznamování poskytovateli služeb sdílení dat (podle kapitoly III), a s ohledem na datový altruismus (kapitola IV). Formální odborná skupina bude mimoto podporovat Komisi a radit jí při řízení meziodvětvové normalizace a při přípravě žádostí o strategickou meziodvětvovou normalizaci."*[96].

214. EDPB a EIOÚ konstatují, že nově zřízený Evropský sbor pro datové inovace *„složený ze zástupců příslušných orgánů všech členských států, Evropského sboru pro ochranu osobních údajů, Komise, příslušných datových prostorů a jiných zástupců příslušných orgánů v konkrétních odvětvích"* (čl. 26 odst. 1) by byl pověřen úkoly vyjmenovanými v čl. 27 písm. a) až e)[97], které jsou též významné s ohledem na zpracování osobních údajů.

215. **EDPB a EIOÚ vítají zařazení EDPB jako člena do Evropského sboru pro datové inovace. EDPB a EIOÚ se však domnívají, že ustanovení týkající se Evropského sboru pro datové inovace budou v souvislosti se zpracováním osobních údajů pravděpodobně zasahovat do úkolů a příslušnosti vnitrostátních úřadů pro ochranu údajů a EDPB v oblasti ochrany základních práv a svobod fyzických osob a usnadnění volného pohybu osobních údajů v Unii[98] (zejména s ohledem na širokou škálu úkolů, které jsou podle článku 70 GDPR svěřeny EDPB, mj. poskytovat Komisi poradenství a vydávat pokyny, doporučení a osvědčené postupy, a úkolů, které jsou podle článku 57 nařízení EUDPR svěřeny EIOÚ).**

---

[96] Důvodová zpráva, strana 8.

[97] „Sbor plní tyto úkoly:
a) radí a napomáhá Komisi při rozvíjení ustálené praxe subjektů veřejného sektoru a příslušných subjektů uvedených v čl. 7 odst. 1 **vyřizujících žádosti o opakované použití kategorií dat uvedených v čl. 3 odst. 1**;
b) radí a napomáhá Komisi při rozvíjení ustálené praxe příslušných orgánů při uplatňování **požadavků vztahujících se na poskytovatele služeb sdílení** dat;
c) radí Komisi při **stanovování priorit meziodvětvových norem, které se mají používat a které jsou vypracovány pro použití dat a meziodvětvové sdílení dat**, meziodvětvové srovnání a výměnu osvědčených postupů, pokud jde o odvětvové požadavky na bezpečnost, postupy přístupu, přičemž jsou zohledněny odvětvové činnosti v oblasti
normalizace;
d) je Komisi nápomocen při **zvyšování interoperability dat a služeb sdílení dat** mezi jednotlivými odvětvími a oblastmi, a to v návaznosti na stávající evropské, mezinárodní nebo vnitrostátní normy;
e) usnadňuje spolupráci příslušných vnitrostátních orgánů podle tohoto nařízení prostřednictvím budování kapacit a výměny informací, zejména stanovením metod účinné výměny informací týkajících se postupu oznamování poskytovateli služeb sdílení dat a registrace a sledování uznaných organizací pro datový altruismus."

[98] Viz například čl. 27 písm. a), podle kterého sbor „radí a napomáhá Komisi při rozvíjení ustálené praxe subjektů veřejného sektoru a příslušných subjektů uvedených v čl. 7 odst. 1 vyřizujících žádosti o opakované použití kategorií dat uvedených v čl. 3 odst. 1" (zvýraznění doplněno).

216. **EDPB a EIOÚ proto doporučují v právním textu vyjasnit, že v souvislosti se zpracováním osobních údajů jsou „příslušným orgánem“ dozorové úřady pro ochranu osobních údajů zřízené podle vnitrostátního práva a práva Unie. Kromě toho by mělo být zřejmé, že poskytování poradenství Evropské komisi ohledně záležitostí ochrany údajů a rozvoje důsledných postupů souvisejících se zpracováním osobních údajů nespadá do příslušnosti svěřené Evropskému sboru pro datové inovace, jelikož článek 70 GDPR tyto úkoly výslovně přiděluje EDPB.**

217. **EDPB a EIOÚ rovněž v zájmu přesnosti a právní jasnosti, jakož i zamezení možnému nedorozumění doporučují přejmenovat Evropský sbor pro datové inovace na „Odbornou skupinu Komise pro správu dat“ nebo podobným způsobem, aby název lépe vyjádřil *právní postavení* a *povahu* subjektu zřízeného podle článku 26 návrhu.**

3.7.4 Článek 31: sankce za porušení návrhu, které mají být uplatňovány

218. **Návrh neharmonizuje sankce za porušení návrhu** (**ani neupřesňuje porušení, která se mají trestat, pokuty za porušení jeho ustanovení, ani orgány či subjekty příslušné k uplatnění takových sankcí**) s tím, že *„[č]lenské státy stanoví sankce za porušení tohoto nařízení a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy o těchto pravidlech a opatřeních uvědomí Komisi nejpozději do [datum použitelnosti nařízení] a neprodleně ji uvědomí o veškerých pozdějších změnách, které se jich dotýkají*“.

219. EDPB a EIOÚ konstatují, že toto ustanovení, omezující vymahatelnost návrhu (schopnost ukládat harmonizované sankce) a případně také podněcující k tzv. „forum shoppingu“ pro nejshovívavější členský stát, je v rozporu s uvedeným cílem návrhu zvýšit důvěru v opakované použití, služby sdílení dat a datový altruismus.

3.7.5 Článek 33: změny nařízení (EU) 2018/1724

220. Tento článek návrhu mění nařízení o jednotné digitální bráně (nařízení (EU) 2018/1724)[99] a zavádí tyto správní postupy: oznámení jakožto poskytovatele služeb sdílení dat, registrace jako Evropská organizace pro datový altruismus. Jejich očekávaný výsledek je: potvrzení o přijetí oznámení, resp. potvrzení registrace.

221. **V této souvislosti EDPB a EIOÚ podotýkají, že režim oznámení a registrace, již analyzovaný v tomto stanovisku, nemůže v zájmu zákonnosti zpracování údajů nahradit nezbytnost vhodného právního důvodu pro zpracování osobních údajů podle čl. 6 odst. 1 GDPR. Jinými slovy, podle GDPR je zpracování osobních údajů zákonné, pouze pokud se uplatňuje vhodný právní základ podle čl. 6 odst. 1 GDPR a pouze v odpovídajícím rozsahu. Návrh by měl tento aspekt jasně upřesnit, aby se předešlo nejednoznačnosti.**

V Bruselu dne 10. března 2021

[99] Nařízení Evropského parlamentu a Rady (EU) 2018/1724 ze dne 2. října 2018, kterým se zřizuje jednotná digitální brána pro poskytování přístupu k informacím, postupům a k asistenčním službám a službám pro řešení problémů a kterým se mění nařízení (EU) č. 1024/2012 (Text s významem pro EHP), Úř. věst. L 295, 21.11.2018, s. 1.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)

Za Evropského inspektora ochrany údajů

Evropský inspektor ochrany údajů

(Wojciech Wiewiorowski)