Západočeská univerzita v Plzni

Fakulta právnická

Katedra ústavního a evropského práva

Diplomová práce

Právní aspekty techniky datapooling v EU

Adéla Strejcová

Plzeň 2024

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Adéla STREJCOVÁ**
Osobní číslo:	**R19M0372P**
Studijní program:	**M0421A220004 Právo a právní věda**
Téma práce:	**Právní aspekty techniky data pooling v EU**
Zadávající katedra:	**Katedra ústavního a evropského práva**

Zásady pro vypracování

Osnova práce
1. Úvod
2. Datapooling jako technika
3. Ochrana osobních údajů
4. Ochrana neosobních dat
5. Manipulace s datapoolem
6. Srovnání s odlišných přístupů v regionech
7. Závěr

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **elektronická**

Seznam doporučené literatury:

- WITZLEB, Normann, PATERSON Moira and RICHARDSON Janice. Big data, political campaigning and the law: Democracy and privacy in the age of micro targeting. Great Britain: Routledge, 2020. ISBN 978-0-429-28865-4
- LUKINGS, Melissa and Arash Habibi LASHKARI. Understanding cybersecurity law and digital privacy: A Common law perspective. Switzerland: Springer, 2022. ISBN 978-3-030-88704-9
- WALTERS, Robert, Leon TRAKMAN a Bruno ZELLER. Data protection law: A Comparative analysis of Asia Pacific and European approaches. Singapore: Springer, 2019. ISBN 978-981-13-8110-2
- EBERS, Martin, Cristina PONCIBO a Mimi ZOU. Contracting and Contract Law in the Age of Artificial Intelligence. Great Britain: Bloomsbury Publishing, 2022. ISBN 978-1-50995-070-6.
- SVANTESSON, Dan Jerker B. Private International Law and the Internet. 3rd edition. Netherlands: Wolters Kluwer, 2016. ISBN 978-90-411-5965-6
- WALTERS, Robert a Marko NOVAK. Cyber Security, Artificial Intelligence, Data Protection & the Law. Singapore: Singer, 2021. ISBN ISBN 978-981-16-1665-5
- CRAIG, Paul and DE BÚRCA, Gráinne. EU law: texts, cases and materials. 7th edition. Oxford: Oxford University Press, 2020. ISBN 978?0?19?885664?1

Vedoucí diplomové práce: **JUDr. Tomáš Pezl, Ph.D.**
Fakulta právnická

Datum zadání diplomové práce: **31. března 2023**
Termín odevzdání diplomové práce: **31. března 2024**

Západočeská univerzita v Plzni
L.S.
Fakulta právnická

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

Doc. JUDr. Monika Forejtová, Ph.D.
vedoucí katedry

V Plzni dne 22. června 2023

Prohlášení

Prohlašuji, že jsem předloženou diplomovou práci na téma: "*Právní aspekty techniky datapooling v EU*" zpracovala samostatně pouze za použití citovaných zdrojů.

V Praze dne 31. 3. 2024 Adéla Strejcová

Poděkování

Na tomto místě bych ráda poděkovala svému vedoucímu diplomové práce JUDr. Tomáši Pezlovi, PhD., který již od roku 2021 trpělivě poskytuje nedocenitelné rady a vede a oponuje mé akademické práce všeho druhu. Dále bych ráda poděkovala Mgr. Filipu Netopilovi a Mgr. Vojtěchu Vrbovi, bez jejichž podpory a odborných rad by tato práce nevznikla. Poslední z mých poděkování patří přátelům a rodině.

Seznam zkratek

ATS	Applicant Tracking System
DDoS	Distributed Denial of Service
DMA	Digital Marketing Act
DGA	Data Governance Act
DPIA	Data Processing Impact Assessment
DPO	Data Protection Officer
DSA	Data Sharing Agreement
DTR	Data Transfer Rate
EHP	Evropský hospodářský prostor
EDPB	European Data Protection Board
SDEU	Soudní dvůr Evropské unie
IaaS	Interface as a Service
ICT	Information and CommunicationTechnologies
IoT	Internet Of Things
IPFS	InterPlanetary File System
NDA	Non Disclosure Agreement
NIS2	
PaaS	Platform as a Service
R&D BER	Research and Development Block Exemption Resolution
SaaS	Software as a Service
SBER	Specialisation Block Exemption Resolution
SLA	Service Level Agreement
TTBER	Technology Transfer Block Exemption Resolution
VABER	
WIPO	World Intellectual property organisation
WP29	Working Party 29 - dnes EDPB
WTO	World Trade Organisation

Obsah

1. Úvod

Žijeme v době, kdy s rostoucí digitalizací, provázanou s rostoucím počtem uživatelů internetu, významně roste i počet dat v digitálním prostředí. Tato data se postupem času stala klíčovými jak pro soukromý, tak i veřejný sektor. Začíná tedy platit, mám informace[1], tedy jsem.[2]

Vhodné zpracovávání dat představuje v soukromé sféře nesmírnou výhodu oproti konkurenci, zejména ve výzkumu a vývoji může znamenat rozdíl mezi technologickým průlomem na straně jedné a neúspěchem na straně druhé. Ve sféře státní správy pak mohou znamenat rozdíl mezi efektivně využitými veřejnými prostředky a zcela nefunkčním systémem.

Data[3] je proto potřeba v některých případech sdílet, v jiných případech zase chránit proti konkurenci. Na jakousi pomyslnou scénu pak přichází datapooly, úložiště dat ke kterým má přístup předem definovaný okruh uživatelů jehož vymezení záleží zpravidla na dohodě mezi vlastníky dat.

Informace získané spojením jednotlivých dat z datapoolu jsou často natolik stěžejní a přelomové, že jejich důsledkem může být poněkud paradoxně jak omezení konkurence, stejně tak i ozdravení trhu a jeho rozšíření možností.[4] Společně s nutností ochrany hospodářské soutěže tak nese rozsáhlé měřítko skladování cenných informací i potřebu zvýšeného důrazu kladeného na kyberbezpečnost. S ohledem na geopolitickou situaci a rozdílné standardy právní ochrany je pak nutné věnovat zvláštní pozornost sdílení dat mimo EHP. Jakýsi

---

[1] Vzhledem k tomu, že pojem "informace" je v právu poněkud nejasný omezuje se autorka v této práci na pojetí informace jako smysly či strojově vnímatelného sdělení, jehož získání má za následek prohloubení a ci naopak snížení (v případě zavádějící informace) poznání stavu okolního světa. Autorka se v tomto směru plně ztotožňuje s názorem, že informaci je možné identifikovat pouze jako změnu v čase. Viz dále například POLČÁK, *Radim. Informace a data v právu*. Revue pro právo a technologie. Roč. 2013, č. 13. ISSN 1805-2797. Strany 74 - 75

[2] Parafráze na citát, jež je přisuzován francouzskému filosofovu, matematiku a fyziku jménem Rene Descartes; *"Cogito ergo sum" - přemýšlím, tedy jsem*.

[3] V právu se vyskytuje pojem data v celé řadě významů, přičemž není možné najít univerzální definici tohoto fenoménu. Prahne-li však laskavý čtenář po explicitní definici, nechť vezme za vděk informací, že pro účely evropského práva považuje autorka v tomto smyslu za nejrelevantnější definici obsaženou v článku 2 odstavci 1 DGA, který data definuje jako "*veškeré digitální záznamy jednání, skutečností nebo informací a všechny soubory takových jednání, skutečností nebo informací, včetně záznamů v podobě zvukové, vizuální nebo audiovizuální nahrávky*".

[4] Poslední jmenované pak zdůrazňuje Unie ve svém Sdělení pod názvem „Směrem ke společnému evropskému datovému prostoru" ze dne 25.4.2018.

pomyslný výčet nejdůležitějších témat pak uzavírá potřeba ochrany osobních údajů.

S ohledem na rozsah práce, se však autorka zaměří pouze na datapooling v soukromé sféře, jelikož právní úprava veřejné sféry je natolik svébytná a problematika natolik rozsáhlá, že by sama o sobě vydala na samostatnou publikaci. Tato práce se rovněž nebude zabývat datapooly ve zdravotnictví, u nichž vyvstávají často zcela jiná etická a právní dilemata nežli u standardních datapoolů. Dalším okruhem, právních vztahů, který bude v této práci cíleně pominut je okruh vztahů vznikajících na základě poolingu dat mezi fyzickými osobami navzájem, který není realizován ve vztahu k vlastní výdělečné činnosti, neboť se jedná o samostatnou okrajovou kategorii, které rovněž zakládají do jisté míry specifické právní vztahy.

Cílem této práce je tedy poskytnout vhled do relativně mladého světa datapoolů a to z pohledu, pro toto odvětví poněkud netradičního - pohledu práva. To celé v kontextu jedné z nejstarších ekonomik - Evropské Unie.

V první kapitole se autorka zaměří na datapooling jako techniku a v krátkosti předestře používané technologie společně s jejich právním přesahem. V následujících kapitolách pak prozkoumá legislativní rámec Evropské unie týkající se ochrany osobních údajů a neosobních dat ve vztahu k datapoolingu. Na závěr práce se pak zaměří na vliv datapoolů na hospodářskou soutěž.

V návaznosti na zadání práce se však autorka nebude zaměřovat na manipulaci s datapooly a srovnání přístupů v mimoevropských regionech, neboť z jejího výzkumu vyplynulo, že se jedná spíše o problematiku zajímavou z hlediska mezinárodního práva, samotná pace však vzniká vzniká na katedře ústavního a evropského práva, pro které není tato problematika v podstatné míře relevantní.

2. Datapooling jako technika

Datapool je tedy strukturalizované centralizované úložiště dat, ve kterém obchodní partneři (a v některých případech i běžní uživatelé[5]) sdílí navzájem svá data a čerpají z něj cenné informace pro své společnosti. Datapool mezi společnostmi je zpravidla zakládán na smluvní bázi, kdy se jednotlivé strany dohodnou zejména na rozsahu sdílení dat a technologiích, které budou za tímto účelem užívány. Jakkoli jednoduše může konstrukce těchto ujednání vypadat,

[5] Pojem uživatel je pro účely této práce chápán jako označení fyzické osoba generující či naopak přijímající data prostřednictvím digitálních komunikačních technologií.

DSA[6] jako smluvní typ, je v praxi jedním z nejsložitějších a nejkomplexnějších druhů smluv vůbec.

Obecně lze pak DSA definovat jako ujednání dvou a více subjektů práva o vzájemném sdílení dat a nebo informací jakéhokoliv druhu mezi těmito subjekty.[7] Tvorba těchto ujednání a potažmo samotného datapoolu s sebou nese celou řadu dilemat, která provází významný právní přesah. Datapool lze totiž zabezpečovat širokou škálou organizačních a technických prostředků. Vyvstávají tak otázky, jakým okruhem subjektů bude datapool tvořen? Budou tyto subjekty uvnitř datapoolu dále hierarchicky strukturovány? Jaký technický prostředek bude s ohledem na bezpečnostně-právní požadavky nejvhodnější a je vůbec takovéto skladování udržitelné? Odpovědi na tyto otázky bude v praxi potřeba řešit vždy s ohledem na konkrétní datapool. V této kapitole kapitole si však rozebereme teoreticko-právní rozměr tohoto problému a poukážeme na některé nečekané právní souvislosti, které mohou nést jednotlivá technická řešení.

2.1 Sdílející subjekty

Již mnohokrát zmiňovaný ekonomický význam sdílení dat, pak přináší různé organizační struktury tohoto sdílení mezi subjekty práva disponujícími daty[8], které lze navzájem dělit podle typů právní osobnosti na subjekty, kterými jsou osoby právnické a na subjekty, kterými jsou osoby fyzické. V praxi tak lze okruhy vztahů vznikající při sdílení dat ve společném datapoolu rozdělit do tří kategorií a sice na situaci, kdy mezi sebou sdílí data dvě právnické osoby, právnická osoba a fyzická osoba a nebo fyzické osoby navzájem.

Vzhledem k rozsahu a zaměření se tato práce, jak již bylo předestřeno v úvodní části, nebude zabývat vztahy, které vznikají mezi jednotlivými fyzickými osobami navzájem.

Co se týče vztahu dvou a více právnických osob, které společně vytvářejí datapool, existují v podstatě dva modely a sice model, kdy mají všechny subjekty stejné postavení a model, kdy je datapool hierarchicky strukturovaný. U modelu kdy mají jednotlivé společnosti vůči sobě stejná a nebo alespoň obsahově obdobná práva a povinnosti nalezneme koncepci DSA, jakožto standardní

---

[6] Z anglického Data Sharing Agreement, volným překladem smlouva o sdílení dat.

[7] VAN ASBROECK, Benoit. Big Data & Issues & Opportunities: Data Sharing Agreements. Online. In: www.twobirds.com. Dostupné z: https://www.twobirds.com/en/insights/2019/global/big-data-and-issues-and-data-sharing-agreements. [cit. 2023-08-08].

[8] Data vlastní a nebo mají oprávnění s nimi disponovat.

multilaterální smlouvy. U složitějších hierarchických struktur pak lze hovořit například o okruhu primárních přispěvatelů, kteří společně uzavírají DSA a třetím stranám nabízejí licencovaný přístup.

Jako jistá forma hierarchického přístupu může být vnímán datapool, ve kterém právnické osoby sdílející generovaná data poskytují licencovaný přístup k vzniklému datapoolu fyzickým osobám. Dalším do jisté míry specifickým podtypem, jsou pak datapooly ve kterých podnikatelé navzájem sdílí vedle určitého okruhu neosobních dat, rovněž osobní data. Právním specifikům takovéhoto sdílení dat se budeme blíže věnovat v kapitole "*Ochrana osobních údajů*".

2.2 Technické prostředky sdílení dat a jejich formát

Informace, jakkoli je ceněna především pro hodnotu sdělení které nese, musí zákonitě mít i svůj hmotný substrát a ve světě ICT i formát. Hovoříme-li tedy o takovéto informaci zachycené v digitálním formátu, hovoříme o datech.

Hmotný substrát pro uchování dat představují různé druhy datových úložišť. Tato úložiště mohou být vlastněna jednou ze smluvních stran, častěji je však pro datapool pronajímána kapacita cloudového úložiště od externího poskytovatele služeb. Z tohoto důvodu je vhodné, aby si již na začátku v samotném DSA strany ujednaly technické prostředky a rozsah přístupu do datapoolu, předpokládanou potřebnou kapacitu, či způsob případného zániku datapoolu a to komu data ze zaniklého datapoolu připadnou. Neméně podstatnými jsou ujednání o financování chodu datapoolu. V následujících kapitolách se proto podíváme na jednotlivé aspekty detailněji.

2.2.1 Místo skladování

Výběr místa skladování je jednou z nejdůležitějších voleb při zakládání datapoolu, která má naprosto zásadní následky pro jeho právní posouzení. V podstatě tak z velké části determinuje to, zda vůbec datapool splní požadavky z hlediska kyberbezpečnosti, například ochrany osobních dat, atd. Jednotlivé způsoby skladování tedy lze rozdělit na umístění datapoolu na serveru jedné ze stran, či na cloudu. Druhý zmíněný způsob skladování pak lze dále rozdělit dle rozsahu externě poskytovaných služeb na řešení typu SaaS, PaaS a IaaS, kteréžto pojmy budou blíže vysvětleny v následujících podkapitolách. Jednotlivé způsoby

skladování se pak často prolínají a je možné je do jisté míry libovolně kombinovat. Výše zmíněné pak může zásadně ovlivnit jurisdikci, které bude datapool podléhat. Toto řešení pak například určí, zda se jej budou týkat pravidla pro předávání (zejména osobních) dat do třetích zemí mimo EHP.[9]

2.2.1.1. Skladování datapoolu na serveru jedné ze stran

Takzvané *in situ*[10] skladování je z právního pohledu nejjednodušším a proti úniku dat nejodolnějším způsobem. Jedná se však o způsob, který bude v drtivé většině případů považován za zastaralý a finančně náročný.

Co se tedy pojmem *in situ* uložení datapoolu znamená? Jedná o situaci, kdy se technická infrastruktura datapoolu nachází v prostorech jedné ze společností sdílejících datapool, přičemž ostatní společnosti pak mají k úložišti vzdálený přístup. Čistě teoreticky si lze rovněž představit situaci, kdy by se data tvořící datapool nacházela vždy v systému té společnosti, která je vytvořila a ostatním společnostem by pak sdílely vzdálené přístupy. Tento systém by však byl nejen uživatelsky nepraktický, ale také by znemožňoval jednoduché, rychlé a účinné kombinování dat v rámci datapoolu, což je však považováno, společně se vzájemným zpřístupněním dat, za hlavní přínos datapoolu.[11] Vzniká tak otázka, zda by takovýto teoretický difúzní datapool byl vůbec datapoolem v pravém slova smyslu, či by byl spíše jakýmsi jednodušším druhem z kategorie dohod o sdílení dat (DSA).

Výhodou *in situ* uložení datapoolu je naprostá kontrola nad okruhem osob, které mají přístup k datapoolu. Společnost, na jejíchž serverech je datapool uložen, zná adresně jména zaměstnanců, kteří provádějí údržbu, a má plnou moc nad jejich výběrem a obsahem pracovních smluv z hlediska důvěrnosti. Může zavádět také různá organizační opatření z hlediska údržby datapoolu, která minimalizují rozsah informací, ke kterým mají jednotlivé osoby autorizovaný přístup. Společnosti tvořící datapool si také mohou určit blíže podmínky za jakých bude společnost zajišťující zázemí s daty pracovat. Mezi další výhody rovněž patří fakt, že nedochází k přechodu povinností ochrany osobních dat ze správce na

---

[9] Evropský hospodářský prostor

[10] Z latiny, lze voleně přeložit jako "*na místě*".

[11] Z hlediska efektivity lze takovýto datapool přirovnat k rozptýlené nervové soustavě hlavonožců ve srovnání s nervovou soustavou homo sapiens. Jistě, kupříkladu taková chobotnice ji s úspěchem využívá, ve vzácných případech dokonce i k hádání výsledků fotbalového klání, ale v žádném případě ji nelze považovat za důvěryhodnou oporu v podnikání.

zpracovatele a v tomto smyslu odpadá nejen administrativní zátěž, ale i s tím spojené bezpečnostní riziko.

Nevýhodou tohoto řešení je především nízká flexibilita, nebezpečí ztráty dat a cena. Co se týče nízké flexibility, ta se projevuje zejména tím, že společnost musí dopředu vědět, jaký rozsah dat bude zpracováván a v souladu s tím vybudovat fyzické kapacity serveru. V případě, že by se pak objem skladovaných dat zvýšil, bude potřeba v lepším případě zakoupit dodatečné zařízení, v horším případě přesunou prostory ve kterých se server navhází. Tato migrace je pak velmi nákladná a časově náročná a ve srovnání s flexibilitou cloudového řešení, kdy může dojít ke zvýšení kapacity v řádu sekund, s náklady, které budou zpravidla odpovídat objemu navýšení využívané výpočetní kapacity, naprosto ekonomicky nevhodná. Další nevýhodou je nebezpečí ztráty dat v případě fyzického poškození serveru, které u cloudových řešení zpravidla nehrozí. Další zásadní nevýhodou bývá cena, neboť datapooly, díky velkému objemu zajišťovaných služeb, obvykle disponují lepšími prostředky pro jejich zajišťování, zejména co se týká softwarové infrastruktury (blíže v kapitolách PaaS a SaaS) a mohou si tudíž dovolit zajišťovat technické prostředí datapoolu výrazně levněji. Dalším, v tomto případě spíše faktickým nedostatkem, je riziko spojené s fyzickým držením serverů na kterých se nachází datapool jednou společností, což může být v budoucnosti zneužito jako nekorektní nástroj při sjednávání nového DSA či jeho dodatků a v konečném důsledku vést dokonce k poškození hospodářského postavení ostatních členů datapoolu.[12]

Prakticky tak lze toto řešení doporučit pouze tehdy, kdy je zakládán velmi malý datapool u kterého nelze předpokládat, že se bude významně rozrůstat, a mezi stranami DSA se nachází společnost, která má vybudovány své vlastní rozsáhlé výpočetní kapacity a personální zajištění, jejichž příslušnou část bude ochotna bezplatně, či za symbolickou úplatu, poskytnout. Rovněž pak musí být v technických silách společností aby si veškerá data, která se nacházejí v datapoolu, zálohovaly ve svých systémech. Součástí DSA by pak mělo být ujednání, které stanoví, že v případě ztráty dat z původního úložiště je společnými silami členové datapoolu v určitém časovém horizontu obnoví.

---

[12] Jistě, právní řády jednotlivých členských států disponují právními nástroji, které lze v takovém případě použít. Zejména vymáhání přístupu k datapoolu soudní cestou je však zdlouhavé a v situaci kdy i relativně krátký výpadek v řádu dnů může společnosti v datapoolu ekonomicky poškodit, neefektivní.

2.2.1.2 Umístění datapoolu na cloudu

Při výběru externího poskytovatele kapacit pro datapool, lze druhy poskytovaných cloudových služeb dělit na základě jejich úrovně a rozsahu na IaaS (z angl. Infrastructure-as-a-Service[13]), PaaS (z angl. Platform-as-a-Service[14]) a SaaS (z angl. Software-as-a-Service[15]). Dělící linie mezi jednotlivými druhy však není jasná. Naopak, většinou se při určování druhu služby jedná spíše o evaluaci převažujících aspektů. Z pohledu právní praxe je možné konstatovat, že při určování charakteru daného konkrétního řešení lze s ohledem na technologii pouze poměrně aplikovat pravidla pro jednu z níže popsaných kategorií. Níže proto budou, vzhledem k rozsahu a určení práce pro širokou právně-akademickou veřejnost, alespoň stručně nastíněny jednotlivé typy datapoolingu, podle rozsahu poskytování služeb, společně s uvedením právních a faktických dopadů jednotlivých technických řešení.

2.2.1.3 IaaS

Jedná se o základní úroveň poskytování cloudových služeb, kdy si společnosti pro svůj datapool pronajmou určitou výpočetní kapacitu na serveru poskytovatele, stejně jako kdyby si pronajaly novou výpočetní techniku do svých vlastních prostor. Společnosti si samy zajišťují veškeré softwarové nástroje pro chod datapoolu a instalují si i svůj vlastní způsob zabezpečení vč. tzv. firewallů atp.[16] Na rozdíl od skladování na serveru jedné z nich však skýtá toto řešení několik výhod. Jednou z nejzásadnějších je takzvaná *virtualizace úložiště*, což v praxi znamená, že jednotka, která se jeví laickému uživateli například jako jeden soubor, je ve skutečnosti rozdělena do mnoha komponent, které se nacházejí na navzájem funkční naprosto oddělených počítačích v rámci jednoho a nebo dokonce více, serverech.[17]

---

[13] V volném překladu “infrastruktura jako služba”.

[14] V volném překladu “platforma jako služba”.

[15] V volném překladu “software jako služba”.

[16] MILLARD, Christopher. Cloud Computing Law. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 32

[17] Více například https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-virtualization a nebo MILLARD, Christopher. Cloud Computing Law. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 33

Tato technika rovněž zlepšuje tzv. *škálovatelnost*[18], Virtualizovat lze rovněž počítač v rámci interního serveru jedné ze společností, ale rozdělení do více serverů přináší daleko spolehlivější ochranu například před živelnými pohromami apod.

Další velkou výhodou, zejména ve vztahu k osobním údajům, je, že jsou data stále zpracovávána za pomocí interních softwarových a lidských zdrojů a provozovateli cloudu, na kterém se datapool nachází tak nevzniká status zpracovatele osobních údajů ve smyslu článku 4 odst. 8 GDPR.[19]

Nevýhodou tohoto řešení je, že si společnosti vytvářející datapool musí zajišťovat veškeré softwarové zázemí a tím i lidské zdroje, které jej vytvářejí a následně udržují v provozu. Toto řešení tak bude dostupné pouze větším datapoolům a to zejména těm do kterých budou přispívat střední a velké společnosti. Nebude tak vznikat nepoměr mezi vynaloženými prostředky a objemem zpracovávaných dat.[20]

Obecně je tedy IaaS jako cloudové řešení pro datapool vhodné zvolit v případech, kdy je například vzhledem k oboru a požadavkům nutné volit velmi specifické řešení a zároveň je potřeba splnit určité velmi úzce definované bezpečnostní požadavky. V takovýchto případech rovněž vyvážená vysoká pořizovací a provozní cena takovéhoto řešení.

2.2.1.4 PaaS

Oproti předchozí kategorii disponuje PaaS zajištěným úplným vývojovým prostředím. Kromě, serveru, úložiště a sítě tak navíc poskytují všechny základní nástroje pro nasazení aplikace, která bude zajišťuje konkrétní prostředí a funkcionality datapoolu. V závislosti na konkrétním druhu PaaS tak

---

[18] Technika v rámci níž je informace rozdělena na části, které lze jednoduše přesouvat a replikovat mezi jednotlivými počítači na serveru a nebo dokonce mezi servery. V případě výpadku jednoho z nich tak lze chybějící komponentu pro určitou informaci nahradit ze zbývajících částí. Díky lze navíc zvýšit výpočetní výkon tím že systém reaguje přidáváním nebo ubíráním zdrojů na nichž jsou jednotlivé komponenty uloženy.

[19] Provozovatel cloudu tak v režimu IaaS nemusí plnit pravidla pro zpracovatele osobních údajů viz zejména čl. 28 GDPR.

[20] Pokud by tyto služby byly sjednány externě, museli by být tito zaměstnanci ve stejném množství a nad rámec těchto nákladů by datapool musel hradit marži provozovateli cloudu.

bývají poskytovány různé úrovně nástrojů nutných pro sestavení, testování, nasazení a správu konkrétní aplikace.[21] [22]

Ve své podstatě si tak datapool v rámci ToS ujedná s poskytovatelem cloudové služby základní úroveň poskytovaných softwarových služeb, které zajistí chod datapoolu a samotný koncový software a jeho údržbu si již zajišťuje sám. Jedná se tak o kompromis z pohledu zajištění základního a obvykle i mnoha dalšími zákazníky prověřeného softwearu, který vytvoří solidní základ pro koncovou aplikaci, která utvoří uživatelské rozhraní s nímž budou jednotliví členové datapoolu pracovat při nahrávání a dílení dat v datapoolu. Tento přístup má hned několik výhod.

Nejzásadnější výhodou je jeho cena, a spolehlivost řešení. Datapool totiž platí nejen za pronájmu výpočetní kapacity na úložišti ale i za používání základních softwarových řešení, která jsou vyvinuta přímo na míru datacloudu. Provozovatel datacloudu si pak vzhledem k tomu, že je provozování cloudu hlavní a nebo jedna z hlavních činností, může a dokonce i musí dovolit investovat významné finanční prostředky do vývoje těchto pro datacloud základních softwarových řešení. Náklady na vývoj tohoto softwaru se pak rozdělí mezi zákazníky, kteří toto řešení používají a nenese je výlučně datapool. Další výhodou je spolehlivost, protože s ohledem na počet zákazníků používajících datacloud je toto řešení zpravidla odzkoušeno v praxi, v případě technických chyb pak může personál, který se zabývá výlučně správou jednotlivých částí cloudu rychle a kvalifikovaně reagovat. Aby byl seznam výhod tohoto řešení kompletní, je vhodné rovněž zmínit fakt, že PaaS bývají obvykle velmi dobře škálovatelné, reagují flexibilně na poptávku po výpočetní kapacitě[23], zároveň si ale zachovávají svobodu volby koncového softwarového řešení datapoolu a proto bývají i velmi bezpečné. Datapool si totiž sám zajišťuje jaké koncové softwarové řešení použije. Může tak zvolit jakýkoli obecně dostupný software a nebo si zadat vývoj vlastního, stále si tak rozhoduje například o tom jaké techniky šifrování dat budou

---

[21] MICROSOFT CORPORATION INC. *Co je PaaS? Platforma jako služba*. Online. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-paas. [cit. 2024-03-31].

[22] *SaaS, PaaS & IaaS Agreements Lawyers & Attorneys*. Online. Dostupné https://www.priorilegal.com/contracts/saas-paas-and-iaas-agreements z: [cit. 2024-03-31].

[23] Blíže například MILLARD, Christopher. Cloud Computing Law. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 37

použity, či jaká bude vnitřní organizační struktura cloudu, nebo jak budou udělovány přístupy.

Nevýhodou jsou jisté omezení z hlediska šíře možností, které se programátorovi z hlediska softwarových nástrojů nabízí a to zejména i možností ohledně kyberbezpečnosti. Tato negativa však mohou být do značné míry účinně omezena výběrem vhodného poskytovatele cloudu. Dalším negativem jsou určitá smluvní omezení z hlediska toho, že větší provozovatelé větších PaaS cloudů obvykle uzavírají své vlastní standardizované ToS, které mohou být pro konkrétní datapool nevhodné. Co se týče hlavních nevýhod je třeba stejně jako na straně výhod zmínit cenu, protože ta je stále v součtu ceny za cloudové služby a za vývoj nebo získání licence k koncovému softwaru ve srovnání se SaaS vyšší.

Tento druh služeb tak budou volit zpravidla střední a větší datapooly, pro něž se bude jednat o cenově výhodné řešení, které ale nabízí dostatečnou flexibilitu a to jak z pohledu výpočetní kapacity a škálování, tak z pohledu volnosti volby konkrétního konečného řešení a možnosti zvýšení úrovně kyberbezpečnosti například z pohledu volby šifrovacích technik či vhodné struktury.

2.2.1.5 SaaS

Poslední a nejkomplexnější úrovní služeb, které může datapool od poskytovatele cloudových služeb získat, je SaaS. V tomto případě provozovatel cloudu poskytuje datapoolu veškerá softwarová řešení, která potřebuje ke svému řešení fungování.[24]

Velkou výhodou je zejména cena a rychlost s jakou datapool může začít fungovat. Není totiž nutné jakékoli vývoj softwaru a datapool může začít fungovat v podstatě momentem podepsání smlouvy s poskytovatelem cloudových služeb. Odpadá nutnost kontrakce dalšího personálu nad rámec běžného fungování společnosti.

Nevýhodou tohoto řešení je nedostatek možností personalizace, který zapříčiňuje i nemožnost přijetí některých dodatečných bezpečnostních opatření, která by jinak strany datapoolu vzhledem k citlivosti skladovaných dat ocenily. Další nevýhodou a hrozbou zejména pro důvěrnost dat fakt, že k nim v určitém

[24] Příkladem společností, poskytující SaaS pro datapooling je například POOL. Online. Dostupné z: https://www.pooldata.io/about-us [citováno dne 11.11.2023]; či společnost COMMPORT, Online. Dostupné z : https://www.commport.com/global_data_synchronization_network/ [citováno dne 11.11.2023]

rozsahu má poskytovatel přístup (viz. Níže kapitola, kterou jsem doposud nepojmenovala). Dalším problémem pak mohou být ToS, které jsou v tomto případě zpravidla pevně dané a není prostor pro vyjednávání odchylných podmínek. Z hlediska zpracovávání osobních údajů je pak nutné brát v potaz nutnost případného uzavření smlouvy s provozovatelem datacloudu jako zpracovatele osobních údajů.

SaaS tak budou volit zejména menší datapooly a datapooly, které nebudou obsahovat vysoce citlivé informace a pro které bude úspora času a financí.

2.2.2. Přenosová rychlost a routing dat

Přenosová rychlost, zkracovaná též jako DTR (z angl. Data Transfer Rate) je rychlost za kterou jsou data přenesena z místa A na místo B, v našem případe z úložiště kde se nachází datapool k jedné ze smluvních stran. Tato rychlost je obvykle udávána v bitech za sekundu. Vzorec výpočtu přenosové rychlosti je $DTR = \frac{D}{T}$, kdy D reprezentuje množství přenesených dat, zatímco T je čas[25] ve kterém jsou tato data přenesena. Jenom pro úplnost je vhodné zmínit, že u úložišť sledujeme v závislosti na druhu dva popřípadě tři parametry, a sice přenosovou rychlost při stanování, nahrávání a popřípadě i synchronizaci.

DTR cloudového úložiště a nebo severu společnosti na kterém se datapool nachází má vliv nejen na na rychlost jak se jednotliví uživatelé v rámci smluvních společností budou schopni získat svá data, ale rovněž na to kolik takových uživatelů se bude schopno připojit. Při určování potřebné přenosové rychlosti je totiž potřeba uvědomit, že maximální D všech přenesených dat z datapoolu je určováno dohromady pro všechny uživatele. Průměrnou DTR pro jednotlivého uživatele (nazývejme ji například DTR_u) tak vypočteme tak, že vydělíme celkovou DTR množstvím uživatelů (N_u) připojených v dané časové jednotce (T) $DTRu = \frac{(\frac{D}{T})}{Nu}$.

V DSA je tedy od začátku potřeba počítat s předpokládaným počtem smluvních stran a množstvím uživatelů, kteří se budou v rámci smluvních stran připojovat. Pozdější rozšíření kapacity či zrychlení DTR je totiž mnohdy komplikované a není vyloučena ani nutnost přesunu celého datapoolu jako mezní

[25] Tento čas je obvykle udáván v sekundách.

řešení, které je ovšem vzhledem k aktuálním cenám za přenosu jednoho TB dat nanejvýš nežádoucí.

Náklady na přenos dat mohou vznikat rovněž díky distribuci dat ukládaných na serverech co nejblíže koncových uživatelů. V praxi jde o to, že provozovatel cloudového uložiště mapuje, která data, jsou jakou skupinou uživatelů cloudu nejčastěji využívána a přesune je na ten ze serverů, který je uživatelům nejblíže. Aby toto uložení mohl dosáhnout, rozmnoží data do více kopií tak aby mohla být uložena co nejblíže určitým skupinám uživatelů. Z právního hlediska nese tato praxe několik nevýhod zejména pokud se nacházejí jednotlivé servery v jurisdikcích různých členských států Unie. Jako zcela nevhodé je nutné toto řešení klasifikován v případě, kdy se některé ze serverů nacházejí mimo Unii.[26]

2.3 Proces validace dat

Jak již bylo řečeno, hodnota datapoolu přímo úměrně souvisí s kvalitou dat, která jsou do něj uložena. Součástí precizního DSA by proto měl být i efektivní mechanismus kontroly, který zajistí, že data nahraná do cloudu budou splňovat předem dohodnuté smluvní limity. Přesto, že validace jako taková není dosud v Unijním právu definována, lze ji pravděpodobně vnímat analogicky s úpravou Spojených států amerických jako "*přezkoumání informací, údajů a postupů s cílem určit, do jaké míry jsou přesné, spolehlivé, nezkreslené a v souladu se standardy pro sběr a analýzu údajů*."[27]

Validace dat pak zpravidla probíhá v závislosti na původu dat v jedné a nebo ve dvou rovinách. První neměnná je kontrola dat systémem pro validaci, který mimo jiné kontroluje zda jsou data kompletní, zadané hodnoty spadají do rozmezí ve kterém se reálně mohou pohybovat a zda nejsou data duplicitní. Poslední zmíněné má pak obzvláště klíčový význam pro efektivitu využití kapacity výpočetního úložiště.[28]

---

[27] Code of Federal Regulations, Title 42, §438.320 pojem "Validation"

[28] Tento koncept je rovněž znám pod zkratkou ISP (In-Situ processing), v praxi jde o to že zejména claudová úložiště ale třeba i bezpečnostní kamery samy provádějí část operací potřebných pro zpracování dat, čímž částečně odpadá potřeba energeticky náročných přesunů z úložiště a zpět podrobněji např. *Cloudové výpočetní úložiště aneb kapacita i výkon na jednom místě*. Online. In: www.cestadocloudu.cz. Dostupné z: https://www.cestadocloudu.cz/blog/cloudove-vypocetni-uloziste-aneb-kapacita-i-vykon-na-jednom-miste/. [cit. 2023-08-08].

Druhá rovina, specifická pro data v jejichž zpracování hraje roli fyzická osoba, je pak vyškolení zaměstnanců jaké mechanismy a postupy dodržovat při kontrole dat předtím než budou tato nahrána do datapoolu.

V rovině softwarové kontroly se nabízí přijetí jednotného validačního softwarového řešení, které bude neoddělitelně včleněno do procesu nahrávání dat na cloud jako jakási vstupní kontrola. Tímto řešením se tak zajistí konzistentní kvalita dat pocházejících od různých stran DSA.

O něco problematičtější je však rovina druhá a sice přijetí kontrolních mechanismů a procesů které budou následovat samotní zaměstnanci společnosti. Tento krok je totiž neoddělitelně spjatý s vnitřní datovou kulturou každé jednotlivé společnosti. V zásadě není možné očekávat od společnosti, kde se zaměstnanci obecně neztotožňují ani se základními pravidly kyberbezpečnosti, jako je střídání hesel nebo odhalení phishing v emailu, aby byli schopni docenit význam přesnosti dat pro dataset. Představu, že zaměstnanci budou dodržovat předepsaný proces u něž nechápou jeho význam, jenom protože je to jejich povinnost, je tak rovněž jaksi mimo realitu.

S vědomím, že důvěrnost a kvalita celého datapoolu je pouze tak dobrá jako nejslabší společnost která do něj přispívá svými daty je proto vhodné do DSA zahnout povinnou smluvní frekvenci školení, či tam kde je to vhodné zejména s ohledem na geografickou polohu a strukturu společností i jednotnou školící instituci či dokonce osobu. Na straně druhé je nutné stanovit smluvní pokutu za nedodržování povinností jak ohledně školení a postupů při validaci.

Na druhou stranu není vhodné zavádět smluvní pokutu tam kde by se jednalo sdílení informací ohledně bezpečnostních incidentech či většiny interních pochybeních týkajících se dat skladovaných v Datapoolu. Je totiž v zájmu věci sdílejících řešit tyto problémy co nejefektivněji a ve vzájemné spolupráci aby se minimalizoval ekonomický dopad na všechny subjekty které data společně sdílejí. Při včasné informaci o chybě, včetně rozsahu a oblasti, které se dotkla, může ovlivnit rozhodování jednotlivých subjektů sdílejících datapool a předejít tak větším ekonomickým ztrátám subjektů sdílejících datapool.

2.3.1 Obecně k vlastnictví dat a jejich nahrávání na cloud externího poskytovatele služeb

Co se týče vlastnictví dat na cloudu u řešení typu IaaS se postačí ujistit, že smlouva ve svých ToS stanoví, že data a software nahraný společnostmi

tvořícími datapool stále náleží dotyčným společnostem a nikoli vlastníkovi hmotného substrátu. Jedná se sice v jistém směru o ustanovení obsolentní, neboť nelze dovozovat, že by data pouhým nahráním na pronajatý hardware měnila majitele. Ve vztahu k poněkud těžkopádné interpretaci dat jako věci v právním slova smyslu a informací jako takových je však takovéto ujednání rozhodně na místě.[29]

Co se týče komplexnějších konstrukcí datapoolů je vždy vhodné se ujistit jaké podmínky jsou v ToS stanoveny a v případě jejich nevhodnosti vyhledat jiného poskytovatele datacloudu a nebo u velkých datacloudů, které budou mít zpravidla lepší vyjednávací pozici, ujednat zcela personalizovanou smlouvu. U ToS je vhodné sledovat nejen vlastnictví primárních dat, které společnosti vědomě nahrají do datacloudu ale rovněž i metadata o uživatelských aktivitách společností.

2.3.2 Technické prostředky ochrany specifických skupin dat v datapoolu

S ohledem na maxima obsažená v NIS 2 a DORA je pak více než vhodné zohlednit rovněž určitá ekonomický rizika například v oblasti know how a patentového práva za účelem ujištění se že tato data nebudou ohrožena. Ku příkladu při poskytování cloudových kapacit úložiště pro datapool třetí stranou, je vhodné aby strany smlouvy zavedly řešení typu IaaS a nebo PaaS společně s vlastním šifrováním v případě, že by byla data natolik zásadní a citlivá, že by za a) vyšší finanční náklady odpovídaly benefitům ze snížení bezpečnostního rizika a nebo za b) vždy, když je důvodné podezření, že by si poskytovatel cloudu mohl využívat know how pro svoje vlastní aktivity. Při volbě řešení typu SaaS je totiž značně zhoršena pozice z níž mohou společnosti kontrolovat, zda provozovatel cloudu nevyužívá informace rovněž pro svůj prospěch.[30] Pokud se však společnost z důvodu nižší citlivosti dat a úspory finančních prostředků rozhodne pro SaaS, je vhodné volit takové poskytovatele, kteří splňují normu ISO 27001, jejíž získání je dobrým praktickým ukazatelem důvěryhodnosti poskytovatele a

[29] Problematiku právního rámce informace a dat blíže například prof. Polčák v dnes již legendárním článku trefně glosuje a přirovnává regulaci k regulaci letového provozu prasat POLČÁK, *Radim. Informace a data v právu*. Revue pro právo a technologie. Roč. 2013, č. 13. ISSN 1805-2797.

[30] Nemusí při dat ani k úniku dat mimo cloud.

kvality jeho vnitřních procesů.[31] Co se týče formální stránky tohoto problému je vhodné explicitně včlenit do TOS určitou formu NDA pamatující na výše uvedený případ, bez technických řešení se však možnost odhalení jednání v rozporu s takovýmto NDA blíží nule. Sami poskytovatelé cloudových služeb pak často přenášejí odpovědnost za ochranu důvěrných informací uživatelů tím, že jim v ToS ukládají zajistit si ochranu svých dat šifrováním[32] (to vše samozřejmě na náklady uživatele, kterým je pro potřeby této práce datapool).

Na závěr obecného úvodu ochrany dat datapoolu skladovaných na cloudu je pak vhodné rovněž zmínit, že i přes jistou neekonomičnost je vhodné krom datapoolu, kde jsou data sdílena, je paralelně zálohovat prostřednictvím uložení na interních informačních rozhraní jednotlivých společností. Poskytovatelé cloudových služeb totiž obvykle neručí za jejich případnou ztrátu.[33]

Co se týče kategorií vlastněných dat, bude nutné vzhledem k neucelené povaze přístupu k datům a informacím rozdělit je na jednotlivé podkategorie. První kategorií kterou si rozebereme ve speciální kapitole je skladování osobních dat v cloudu. Zde se bude jejich vlastnictví a celková povinnost ochrany odvíjet zcela diametrálně odlišně a to především s ohledem potřeb lidských bytostí a nebo chcete-li fyzických osob o kterých tato data pojednávají.

2.3.2.1 Duševní vlastnictví

V přístupu k právům duševního vlastnictví v datapoolu vznikají jisté problematické body co se týče rozdílného pohledu anglosaského právního systému a kontinentálního právního systému na to co je a není autorským dílem. Zatímco anglosaský právní systém jako autorské dílo uznává všechna díla, k

---

[31] Zde si autorka plně uvědomuje, že ISO 27001 není nikterak právem vyžadováno a jedná s o pouhou technickou certifikaci, tj. poskytovatelé cloudových služeb, kteří se rozhodli o certifikaci neusilovat mohou zajišťovat stejně kvalitní služby ovšem za pomocí jiných technických prostředků než těch které jsou vyžadovány normou. Pro právní jak laickou tak akademickou veřejnost je však splnění normy hodnotným praktickým ukazatelem.

[32] AWS Customer Agreement ve verzi z 27. října 2023 odstavec 2.2. Online. Dostupné z https://aws.amazon.com/agreement/ - [cit. 2023-4-11]

[33] iCloud Terms and conditions Oddíl III. písmeno o). Online. Dostupné z https://www.apple.com/legal/internet-services/icloud/cz/terms.html [cit. 2023-5-11], Dále pak například Microsoft Services Agreement bod. 6 Service Availability *"...Microsoft is not liable for any disruption or loss you may suffer as a result."*

jejichž vzniku byla zapotřebí určitá míra úsilí, úsudku a schopností[34] a hranice mezi tím toho co je a není autorským dílem je stanovována podle míry úsilí, jehož bylo potřeba vynaložit.[35] Kontinentální systém práva, zpravidla požaduje pro uznávání autorských děl určitou míru kreativity. Pro srovnání lze uvést například článek 2 revidovaného znění Bernské Úmluvy. [36] Vzhledem k zaměření této práce se budeme téměř výhradně zabývat právem kontinentálním, jakožto systémem používaným v Evropské Unii, je však vhodné zmínit, že velká část mezinárodních datapoolů bude z důvodů na straně mezinárodního práva soukromého, muset zohledňovat při svém vzniku a fungování i zákazníky či společnosti mimo EU a systém kontinentálního práva.

S Ohledem na existenci celé řady světových právních subsystémů je pak rovněž možné zvolit znění DSA, které bude svým zněním explicitně odkazovat na TRIPS[37] jakožto multilaterální mezinárodní smlouvě sestavené pod hlavičkou WTO. V tomto směru je pak pro kontraktační proces směrodatný zejména článek 10 odstavec 2 TRIPS, který v podstatě svým zněním odpovídá odstavci 5 článku 2 revidované Bernské úmluvy,[38] byť tento hovoří o sbornících literárních děl, encyklopediích a antologiích. S ohledem na historický kontext je však vhodné přijmout teleologickou metodu výkladu s tím, že účelem odstavce 5 článku 2 Bernské úmluvy, je ochrana databází a výčet jednotlivých druhů informačních kompilací se v důsledku významného technologického vývoje stal pouze demonstrativním. Ochranu poskytovanou výše zmíněným článkem tak bude možné poskytnout i takovému uspořádání dat jakým je datapool. V tomto směru je pak nanejvýš argumentace WIPO, která vyslovila názor, že v případě, že by

---

[34] Viz. například Britský autorský zákon Copyright, Designs and Patents Act 1988 článek 3 odstavec 1. V tomto kontextu je nutné zmínit, že Velká Británie byla z důvodu svého začlenění do Evropské Unie mezi lety 1973 a 2016 významně ovlivněna působením kontinentálního systému, což se projevuje i v článku 3 výše zmíněného zákona včleněním písmen a), b), a d), které reflektují Směrnice EU a to konkrétně Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází aSměrnice Evropského parlamentu a 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů

[35] MILLARD, Christopher. Cloud Computing Law. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 204 a 205.

[36] Revidovaná Bernská úmluva o ochraně literárních a uměleckých děl, v ČR dostupná ve vyhlášce Ministerstva zahraničí 133/1980 Sb. ve znění pozdějších předpisů - dále jen Bernská úmluva

[37] Agreement on Trade-Related Aspects of Intellectual Property Rights as Amended by the 2005 Protocol Amending the TRIPS Agreement. Online. Dostupné z: https://www.wto.org/english/docs_e/legal_e/trips_e.htm#part1

[38] Bernská úmluva o ochraně literárních a uměleckých děl ze dne 9. září 1886, Doplněná v Paříži dne 4. května 1896, revidovaná v Berlíně dne 13. listopadu 1908, doplněná v Bernu dne 20. března 1914, a revidovaná v Římě dne 2. června 1928, v Bruselu dne 26. června 1948, ve Stockholmu dne 14. července 1967 a v Paříži dne 24. července 1971

databáze nepodléhaly ochraně ve smyslu odstavce 5 článku 2 Bernské úmluvy, by tyto databáze dat bylo možno vnímat jako autorským právem chráněné dílo ve smyslu odstavce 1 výše zmíněného článku[39], jež stanoví, že.: "*Výraz "literární a umělecká díla" zahrnuje všechny výtvory z literární, vědecké a umělecké oblasti, bez ohledu na způsob nebo formu jejich vyjádření…"* Z dlouhodobé perspektivy pak bez zajímavosti, že tedy případné porušení pravidel týkající se autorských práv datapoolů chráněných TRIPS pak může být předloženo k vyřešení Orgánu pro řešení sporů WTO neboli DSB. Může tak učinit kterýkoliv ze členů WTO, kterými jsou jek jednotlivé signatářské státy tak EU v pozici mezinárodní organizace sui generis[40]. Tento mechanismus[41] pak může[42] být v budoucnu zcela stěžejní pro koncepční řešení sporů vznikajících z exportu dat do datapoolů nacházejících se částečně a nebo zcela mimo Unii a tedy podléhajících částečně jurisdikci států mimo evropskou Unii.

Vraťme se však opět do oblasti ryzího práva Evropské Unie jemuž je tato práce primárně věnována. Zde do obecného rámce autorského práva vstupují dvě směrnice a sice Směrnice o právní ochraně počítačových programů[43] a Směrnice o právní ochraně databází[44].

Začněme nejdříve Směrnicí o právní ochraně databází, která chrání "… *databáze, které způsobem výběru nebo uspořádáním obsahu představují vlastní duševní výtvor autora, chráněny jako takové podle autorského práva*…"[45] Svou povahu poskytuje tato směrnice ochranu uspořádání dat v datpoolu, které vzniklo na základě manažerského rozhodnutí o tom jak budou data organizována. Autorem přitom může být v závislosti na právech jednotlivých členských států

---

[39] WORLD INTELLECTUAL PROPERTY ORGANIZATION. *WIPO publication No. 464 (E) - Implications of the TRIPS Agreement on Treaties Administered by WIPO*. Přetisk 2012. ISBN 978-92-805-0681-1.

[40] Více na příklad EVROPSKÝ PARLAMENT. *Evropská unie a Světová obchodní organizace*. Online. Dostupné z: https://www.europarl.europa.eu/factsheets/cs/sheet/161/evropska-unie-a-svetova-obchodni-organizace. [cit. 2024-02-24].

[41] Podrobněji WTO *Understanding on rules and procedures governing the settlement of disputes.* Online. Dostupné z: https://www.wto.org/english/tratop_e/dispu_e/dsu_e.htm. [cit. 2024-02-24]

[42] To vše za předpokladu, že se WTO podaří vyřešit krizi jejího Odvolacího orgánu, viz. blíže například. *Members told "finish line within reach" in dispute settlement reform talks.* Online. https://www.wto.org/english/news_e/news23_e/dsb_18dec23_e.htm. [cit. 2024-02-24].

[43] Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází

[44] Ibid.

[45] Článek 3 odst. 1 Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází

buď pouze fyzická osoba či skupina fyzických osob, které strukturu datapoolu vymysleli a nebo rovněž právnická osoba, které takové autorské právo svědčí.[46] Vzniklý datapool je pak zpravidla kolektivním autorským dílem.[47] Z pravidla tak bude vznikat model, ve kterém budou jednotlivé zakládající strany DSA, které se podílely na ujednání jejího organizační struktury rovněž autory kolektivního[48] autorského díla. V tomto směru však není úprava autorských práv napříč jednotlivými státy Unie dostatečně harmonizovaná, zvláště z hlediska toho, zda může být právnická oba spoluautorem či autorem a zda její autorství bude nadřazeno autorským právům zaměstnance, který na její pokyn strukturu datpoolu stvořil.[49] Jakýmsi limitem však je tak pouze fakt, že datapool jakožto databáze musí být chráněn právem členského státu v mezích stanovených článkem 3 odst. 1 Směrnice o ochraně databází.[50]

Pro autorství datapoolu je proto v tomto směru určující konkrétní právní řád, kterým se bude DSA řídit. Zejména z pohledu datapoolů vytvářených společnostmi, jež působí ve vícero členských státech pak lze doporučit volbu takového rozhodného práva, které umožní přenést veškerá autorská práva na jednotlivé společnosti, jež budou následně vystupovat jako jednotliví spoluautoři výsledného datapoolu. Takovéto právní uspořádání významně zjednoduší nejen řešení každodenních provozně-právních otázek, ale také zajistí případný bezproblémový převod práv k datapoolu na jinou osobu. De lege ferenda by pak upevnění právní jistoty významně přispěla jednotná celoevropská úprava v této oblasti a to zejména s ohledem fakt, že autorské kolektivy složené výhradně z občanů jednoho členského státu se zejména v obchodní sféře jsou spíše výjimkou.

Ochrana v rámci Směrnice o ochraně databází zahrnuje pouze strukturální uspořádání datapoolů[51] a nelze je aplikovat na data zahrnuta v

---

[46] Ibid. čl. 4 odst 1.

[47] Ovšem za předpokladu, že právní řád členského státu jehož právem se daný stát řídí vznik kolektivního práva připouští srov. Směrnice o ochraně databází čl. 4 odst. 1

[48] Vzhledem k jazyku, kterým je práce psána, považuje autorka za důležité zdůraznit, že pomologie odpovídá oficiálním překladům právních norem Evropské unie, nikoli pak vnitrostátním pojmům používaným v právním řádu České Republiky, zejména zákonem 121/2000 Sb.

[49] KOŠČÍK Michal, MYŠKA, MATĚJ. (2018) Data protection and codes of conduct in collaborative research. *International Review of Law, Computers & Technology* https://doi.org/10.1080/13600869.2018.1423888 Kapitola 2.2.1. Strana 49.

[50] Rozhodnutí o předběžné otázce SDEU Football Dataco ve věci C-604/10 bod 50.

[51] Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází čl. 3 odst. 2

datapoolech, která jsou chráněny zvláštními autorskými právy jako je software a nebo data o vědeckém výzkumu atd. U těchto kategorií dat proto není nutné se obávat toho, že by samotným nahráním na cloud externího poskytovatele docházelo k převodu práv jakýmsi konkludentním jednáním, což ostatně ToS renomovaných poskytovatelů cloudových uložišť akcentují.[52]

DSA ze svojí povahy kontraktu rovněž nemůže normovat vznik autorských práv jako takový, ale pouze deklarovat a nebo pro futuro stanovit jaký podíl tvůrčí činnosti při vzniku datapoolu jednotlivé strany vynaložily a nebo vynaloží.

Dalším problematickým aspektem ve vztahu k autorství datapoolu jako databáze je možné rozšíření počtu stran podílejících se na datapoolu nad rámec původního okruhu členů, který datapool založili. Z tohoto pohledu pak zásadně nebudou nově přistoupivší členové těžit z autorských práv v rozsahu strukturálního uspořádání databáze, bude jim však svědčit tzv. Zvláštní právo, které umožňuje pořizovateli databáze, zabránit vytěžování a nebo zužitkováním celého obsahu databáze a nebo jeho kvantitativně či kvalitativně podstatné části[53]. Jako vytěžování je přitom chápána jakákoliv forma trvalého nebo dočasného přenosu významné části datbáze[54], představované v tomto případě datapool. Oprávněný uživatel datapoolu - tj. uživatel, který přistupuje k datům na základě otevřeného přístupu, pokud datapool tento přístup umožňuje, může libovolně zužitkovat kvalitativně a kvantitativně nepodstatné části.

Zvláštní právo je v tomto smyslu koncipováno jako ochrana investic do datapoolu v rozsahu, ve kterém jejich vklad zvýšil kvalitativní a kvantitativní hodnotu datapoolu. Vklad přitom může spočívat jak ve vynaložení finančních prostředků, ale také "*času, práce a energie*[55]" Jakkoli však mají odůvodnění v systému evropského práva vysvětlující účel, výše zmíněný text chápání účelu

---

[52] Viz více například Google Drive Additional Terms of Service, kapitola 1 "*…your content remains yours. We do not claim ownership in any of your content, including any text, data, information, and files that you upload, share, or store in your Drive account"* citováno dne 5.11.2023 dostupné z https://www.google.com/drive/terms-of-service/. Dále například Dropbox Terms of Service kapitola Your Stuff & Your Permissions, která uvádí "*Your Stuff is yours. These Terms don't give us any rights to Your Stuff except for the limited rights that enable us to offer the Services." Citováno dne 5.11 2023, dostupné z https://www.dropbox.com/terms.*

[53] Čl. 7 odst. 1 Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází

[54] Ibid. čl. 7 odst. 1 písm a)

[55] Ibid. Odstavec 41 odůvodnění

normy přináší spíše otazníky[56]. Pro účel této práce se však spokojme s vysvětlením, že nejvhodnější je rozsah autorství nového člena specifikovat přímo v DSA, tak aby zůstala zachována všechna právními předpisy garantovaná práva a zároveň byla vytyčena jasná dělící linie.

Výjimkou z tohoto pravidla je pak užití dat pocházejících z datapoolu pro účely názorné výuky a vědeckého výzkumu v rozsahu, který je odůvodnitelný nevýdělečným cílem.[57],[58] Další výjimkou je užití datapoolu pro účely veřejné bezpečnosti nebo správního či soudního řízení.[5960]

Pro úplnost je vhodné zmínit, že zvláštní práva pořizovatele chrání databázi jako součást datapoolu patnáct let od 1. ledna roku následujícího po dni zhotovení databáze. Přičemž tuto dobu ochrany lze považovat v současném dynamicky se vyvíjejícím oboru IT za dobu dostatečnou, ne-li přehnanou.[61]

Dalším aspektem doplňujícím ochranu technických aspektů datapoolů je ochrana softwaru, který v rámci datapoolu umožňuje sdílení data, popřípadě data organizuje a generuje derivativní informace. Tato úroveň ochrany pak bude stěžejní zejména pro datapooly, in situ a nebo externí cloudové služby až do úrovně PaaS. Datapooly využívající cloudových služeb typu SaaS si totiž veškeré softwarové zázemí pronajímají.

Středobodem harmonizované ochrany v této oblasti je Směrnice o ochraně počítačových programů,[62] tato směrnice podobně jako směrnice o

---

[56] Samotná formulace "*vynaložení času, práce a energie*" je problematická. Kupříkaldu není jasný výklad slova energie, může se tak jednat stejně dobře o energii elektrickou, která umožňuje skladování, z pohledu obecného jazyka českého by se však nabízel spíše výklad, který slovo "energie" vnímá jako synonymum lidského úsilí. Proti tomu však hovoří anglické znění směrnice ve kterém se hovoří o effort, což lze přeložit jako úsilí či snaha, v českém znění je však slovo effort nahrazeno slovem práce.

[57] Je vhodné podotknout, že tato hranice je velmi těžko určitelná, zejména v situaci, kdy je různá forma spolupráce veřejných i soukromých center a univerzit s komerčním sektorem pro financování výzkumu stěžejní.

[58] Článek 9 písmeno b) Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází

[59] Na tomto místě je vhodné podotknout, že toto pravidlo je nutné vykládat velmi restriktivně, vzhledem k možným ekonomickým následkům úniku dat o přesné struktuře databáze, který je nevratný. Veřejné instituce pak nemají velmi často dostatečné prostředky jak tato data efektivně chránit.

[60] Článek 9 písmeno c) Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází

[61] Lze se domnívat, že takto dlouhá ochrana databází byla zákonodárcem stanovena zejména díky faktu, že první znění této směrnice bylo schváleno již v roce 1996, tedy v době, kdy technologický vývoj v oboru informačních technologií nebyl tak turbulentní jako je dnes.

[62] Směrnice Evropského parlamentu a 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů

ochraně databází poskytuje ochranu autorskému dílu[63], které stvořila osoba a nebo skupina osob. Narozdíl od své starší sestry však jasně stanovuje možnost vytvoření autorského díla v zaměstnaneckém režimu, kdy veškerá práva nabývají společnosti, na jejichž pokyn zaměstnanec dané softwarové řešení pro datapool vytvořil.[64] Ochrana je přitom poskytována vyjádření programu v jakékoliv formě, což mimo jiné zahrnuje: "*Myšlenky[65] a zásady, na kterých je založen kterýkoliv z prvků počítačového programu včetně myšlenek a zásad, na kterých je založeno jeho rozhraní, nejsou chráněny autorským právem podle této směrnice.*" Tento koncept autorství softwaru je pak velmi důležitý zejména v situaci, kdy jsou data poskytnutá členy cloudu dále zpracovávána některou z technik strojového učení,[66] spojených se vznikem derivativních dat[67].

2.3.2.2 Obchodní tajemství

Přesto, že z pohledu obecné etiky by se mohlo zdát, že zachovávání důvěrnosti a obchodního tajemství je automatickou součástí analogicky k zákonné povinnosti zachovávat listovní tajemství v digitální komunikaci. Opak je ale pravdou. V praxi je tedy nutné v případě uzavírání služby s poskytovatelem cloudové služby typu SaaS[68] uzavřít jako ToS i NDA a to v co nejkonkrétnějším znění, které krom obecného závazku nepoužívat jakákoliv data která jsou nahrána do datapoolu rovněž explicitně stanoví závazky týkající se obchodního tajemství.

Součástí ToS a potažmo i NDA by měl být i zákaz jiné než nezbytné získávání a jakéhokoli externího používání derivativních dat o datapoolu. Derivativní data jsou v tomto případě data, která vytváří provozovatel datacloudu na základě uživatelské aktivity zaměstnanců společnosti tvořící datapool při používání datapoolu. Jakkoli se tento fenomén na první pohled může zdát nevýznamný, opak je pravdou. Někteří poskytovatelé služeb datacloudu totiž

---

[63] Směrnice Evropského parlamentu a 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů článek 1 odst. 1

[64] Článek 2 odst. 3 Ibid.

[65] Zde je potřeba podotknout, že textace českého znění je v tomto případě mimořádně nešťastná. Přikloňme se tedy spíše k vyjádření v anglickém znění, které používá slovo "idea", které lze do češtiny přeložit spíše jako "nápad". Pokud bychom totiž trvali na doslovném výkladu "myšlenky", dostaneme se v kontextu normy do rozporu s článkem 10 Listiny základních práv Evropské unie

[66] Jednou z technik strojového učení je i umělá inteligence.

[67] Data vzniklá na základě kombinace a nebo vyhodnocení již existujících dat za pomocí algoritmu.

[68] Toto maximum se může v omezené míře vztahovat i na PaaS v závislosti na druhu a rozsahu poskytovaných služeb poskytovatelem datacloudu.

automaticky počítají se ziskem, který utrží z monetizace vytěžených derivativních dat a nabízejí tak nižší ceny[69]. Z takovéto praxe však datapool profituje pouze v krátkodobém horizontu. V tom dlouhodobém pak může být mapováno množství informací v datapoolu, uživatelské zvyky zaměstnanců v jednotlivých společnostech tvořících datapool nebo třeba i pokrok ve výzkum v jednotlivých společnostech na základě objemu nově nahrávaných dat. Takováto praxe pak může mít naprosto hrozivé výsledky co se týče znevýhodnění postavení společností tvořící datapool na poli hospodářské soutěže. Poskytovatel cloudových služeb by pak rovněž měl být nejlépe prostřednictvím explicitního ustanovení v ToS zavázán k tomu, aby přijal odpovídající zabezpečení skladovaných dat. Zde ovšem znovu platí, že solidní poskytovatel bude na kvalitu a věrohodnost svých služeb hledět automaticky[70] bez potřeby dalšího ustanovení. Dalším velmi důležitým aspektem ToS je rovněž ujednání za jakých podmínek a zda vůbec může poskytovatel cloudových služeb zadat část poskytování třetím stranám jako svým smluvním dodavatelům.

V případě IaaS a PaaS je pak na společnostech vytvářejících DSA aby si zvolily účinnou kryptografickou techniku.[71] V takovém případě budou v Cloudu skladována data, která ale nebude mít poskytovatel možnost kvalitativně číst a rozlišovat v nich jednotlivé kategorie.

2.3.2.3 Patenty a ochranné známky

Co se týče datapoolem užívaných patentů a ochranných známek, je vhodné si zajistit kromě patřičných licenčních oprávnění, kterými se budeme zabývat v kapitole Rozsah sdílení informací a jejich použití i explicitní NDA za strany poskytovatele cloudových služeb. Přestože část právní veřejnosti jejíž zástupcem je například Millard,[72] je toho názoru, že zveřejněním obsahu konkrétního patentu či konkrétní ochraně známky by se poskytovatel dopouštěl v praxi ekonomické sebevraždy a proto není takovýto únik dat pravěpodobný, nelze než tento názor rezolutně odmítnout a to jak pro potřeby cloudů o kterých Millard

---

[69] MILLARD, Christopher. *Cloud Computing Law*. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 212

[70] MILLARD, Christopher. *Cloud Computing Law*. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 214

[71] Blíže například - Suniany university in Ghana https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10484459/pdf/pone.0290831.pdf

[72] MILLARD, Christopher. *Cloud Computing Law*. Oxford University Press, 2013. ISBN 978–0–19–967168–7. Strana 220

konkrétně pojednává tak pro potřeby datapoolingu a tedy i účel této práce. Millardův argument pro toto tvrzení, je v zásadě ten, že v momentě kdy by zákazník zjistil, že ze strany datacloudu unikla citlivá data jeho konkrétním jménem, bylo by prakticky jisté že by automaticky začal vymáhat odškodnění a nápravu a že u poskytovatele SaaS v praxi nedochází k právním specifikům oproti běžnému v porušení ve fyzickém světě. Tento postoj však naprosto nezohledňuje měřítko zpracování dat a fakt, že i když unikne specifický a jmenovitě určený obsah, možnosti jak únik vysledovat k poskytovateli datacloudu a rovněž jej prokázat je velmi omezené množství. Připočtěme pak fakt, že z důvodu geopolitické situace není vůbec jisté zda se o úniku konkrétního licencovaného materiálu kupříkladu na asijský trh společnosti vytvářející datapool vůbec dozví.[73] Oproti standardním opatřením proti úniku patentu z on-site výpočetní techniky ja pak zapotřebí vynaložit vyšší úsilí a zajistit veškeré dostupné prostředky ochrany, jestliže dávají smysl v poměru s ekonomickou hodnotou chráněného obsahu. Oproti standardnímu konceptu odpovídající péče, tak nebudou prováděna pouze dostatečná opatření, ale veškerá dostupná opatření jejichž náklady budou proporcionálně odpovídat chráněné hodnotě.

Dalším velmi odlišným aspektem, který bude důležitý zejména pro datapooly využívající služby PaaS a částečně i SaaS je vymezení si práv k obsahu mezi poskytovatelem kloubové služby a datapoolem. Zde lze z právního hlediska pouze zmínit, že by měl být v ToS co nejpřesněji vymezený. Prakticky je rovněž s ohledem na výše zmíněné ujednání ToS a velikost datapoolu sjednat odpovídající čas na případnou migraci datapoolu a rovněž podmínky podpory této migrace a technické parametry tak, aby bylo případně potřeby možné datapool přesunout.

Další rovinou je ochrana datapoolu

2.4 Rozsah sdílených informací a jejich použití

Rozsah sdílených informací je alfou a omegou samotného účelu DSA. Již na samotném začátku sdílení dat v datapoolu by si měly společnosti položit otázky týkající se množství a kvality dat, kterými budou jednotlivé společnosti do datapoolu přispívat. Toto množství, může být vymezeno jednak druhově jako veškerá neveřejná data týkající se určité problematiky, která jsou jednosltlivým společnosti tvořícím datapool k dispozici. Ale lze jej vymezit i v závislosti na

[73] To že se společnost o úniku jistého licencovaného materiálu nedozví, neznamená, že ona sama anebo poskytovatel tuto skutečnost nepocítí a to například ve formě snížené poptávky ze strany zmíněného geopoliticky izolovaného trhu.

určitém jednání společnosti, kupříkladu ve vztahu ke konkrétním datům, která společnosti získají v průběhu testování či prodeje určitého výrobku a nebo v průběhu interakce s určitou skupinou zákazníků.

Při tvorbě datapoolu je také nutné explicitně sjednat časový horizont v jakém budou data zpřístupňována, samotný fakt že si společnost ponechá data ve svém výlučném držení po delší dobu, totiž může znamenat vytvoření významné informační nerovnováhy a společně s ní i konkurenční výhody.

Dalším pro tvorbu datapoolu významným faktorem je jeho technologické uspořádání. Strany DSA by si proto předem měly jasně vymezit účel za kterým datapool zakládají a přizpůsobit odpovídajícím způsobem jeho architekturu, ale i kapacitu a další technologické aspekty.

Datapooly obecně se mohou zakládat na různých kategoriích struktur v závislosti na způsobu přispívání jednotlivých společností. V zásadě tak existují dvě kritéria dělení, nabízející vždy po dvou způsobech řešení. Datapooly tak lze dělit podle způsobu organizace na datapooly s bez vertikální struktury, ve kterých jsou si všichni členové rovni a na datapooly s vertikální strukturou, kdy někteří členové zaujímají nadřazenou pozici nad dalšími členy datapoolu. Dalším organizačním prvkem a druhým dělením je organizace datapoolu z hlediska veřejnosti, v závislosti na níž dělíme datapooly na datapooly neveřejné, k nimž mají přístup pouze strany DSA a na datapooly veřejné, ke kterým má přístup široká veřejnost, zpravidla se tak děje na základě licence a za úplatu.

2.4.1 Datapooly z hlediska organizačního uspořádání

Prvním a způsobem dělení na který je z hlediska práva vhodné se strukturálně zaměřit je přístup z hlediska rovnosti postavení jednotlivých členů datapoolu.

Toto dělení není vhodné směšovat s horizontálním a vertikálním působení na trhu, které si rozebereme níže, v kapitole o ochraně hospodářské soutěže.

2.4.1.1 Horizontálně organizované datapooly

Tato kategorie datapoolu vyniká za situace, kdy si společnosti v DSA ujednají, že všechny z nich budou přispívat do datapoolu více méně rovným dílem. Určitá nevyváženost objemu dat, kterým mohou jednotlivé strany přispět může být případně kompenzována jistým relativně drobnějším poplatkem, který

však není primárním motivátorem a slouží pouze jako jakási kompenzace. K datapoolu pak nemají přístup třetí strany, které by byly čistými recipienty.

Další fakultativní variantou datapoolu této kategorie může být ujednání o vytvoření technologického datapoolu, kdy strany společně zadají třetí straně provádění výzkumu, který společně financují a jehož výsledky jsou nahrávány do datapoolu, ze kterého následně společnosti data získávají. Toto ujednání je výhodné nejen z hlediska rozdělení nákladů na výzkum, ale také z toho pohledu, že výsledky výzkumu získávají strany ve stejný čas a žádná z nich tak není znevýhodněna. Z hlediska hospodářské soutěže, by pak měly mít všechny strany přístup ke kompletním výsledkům výzkumu aby nedocházelo k protisoutěžnímu efektu.

Tato struktura tak s sebou nese jednak úsporu finanční, tak přístup k informacím, které by jinak společnosti buď vůbec nezískaly a nebo nezískaly v dostatečném množství, což podporuje vývoj nových technologií a v konečném důsledku pa i zlepšení výrobků či služeb, které jsou poskytovány zákazníkovi.

Problematické v tomto směru pak mohou být ale finanční datapooly, ve kterých si finanční společnosti sdílejí informace o kredibilitě zákazníků. Dalším klasickým příkladem jednoduchých horizontálních datapoolů mohou být ve své základní verzi datapooly sdílející informace získané produkty společností v rámci IoT. Klasickým příkladem hovořícím za všechny mohou být informace získané autonomními automobily během jejich provozu. Tyto informace pak mají v tomto konkrétním případě krom výše zmíněného význam i pro obecné zlepšování bezpečnosti a to nejen z hlediska implementace poznatků do výrobků ale do budoucna i obecné bezpečnosti na pozemních komunikacích.

Tuto organizační strukturu ta nejčastěji volí společnosti jejichž primárním cílem je sdílet navzájem informace s podobně ekonomicky postavenými partnery. Tyto společnosti pak velmi často upřednostňují důvěrnost před možností sekundární monetizací údajů pomocí poskytování přístupu k informacím třetím stranám, které nemohou přispět svými daty. Horizontálně organizované datapooly pak zpravidla přiznávají rozhodovací práva co se týče organizačních záležitostí datapoolu všem strom rovným dílem, popřípadě dílem přímo odpovídající podílu na vkládaných datech.

Pro úplnost je pak vhodné zmínit, že horizontálnímu charakteru uspořádání datapoolu nebrání najetí externího správce pro zajišťování technických aspektů fungování datapoolu.

2.4.1.2 Vertikálně organizované datapooly

Tento typ organizační struktury se zakládá na tom, že existuje okruh primárních přispěvatelů, kteří poskytují do datapoolu data a sekundárnímu okruhu uživatelů datapoolu, kteří k těmto datům mají obvykle za úplatu přístup. Fakultativně pak mohou vznikat datapooly u nichž si společnosti přispívající do datapoolu daty zvolí orgán, který bude na základě jejich pokynů datapool organizační spravovat a vznikne tak jakási třetí vrstva této struktury. Dalším možným modelem vertikální organizace je pak založení datapoolu jedinou společností, která je jediným poskytovatelem dat pro datapool a nebo organizuje poskytování dat do datapool dalšími společnostmi, které však podléhají jejím organizačním pokynům. Může se tak dít altruisticky a nebo za úplatu poskytovanou organizační společnosti.

Všechny výše zmiňované modely pak mají společné to, že se na rozhodování o organizačních věcech datapoolu společnosti a další uživatelé datapoolu nepodílí rovným dílem. Část z nich nemá žádnou rozhodovací pravomoc nad směřováním datapoolu a nebo je tato pravomoc velmi omezená. V tomto modelu je tak nutné dohodnou okruh recipientů, kteří budou mít k datapoolu přístup a podmínky tohoto přístupu. Zda se tak bude dít za pomo

Tyto datapooly pak bývají mnohem častěji monetizovány než jejich protějšky s horizontální strukturou. Jejich součástí pak bývá často mnohem různorodější spektrum přispěvatelů a beneficientů s různými zájmy a ekonomickým postavením.

3 Ochrana osobních údajů

Jestliže v rámci ochrany dat existuje skupina, která svým významem vyniká nad ostatní svojí důležitostí, a v návaznosti na to i přísností úpravy, jedná se o data zachycující informace o fyzických osobách. Pokud data určují směřování společnosti a jejich zpracovávání, potažmo držení je jedním z nejcennějším aktiv vůbec, pak jsou osobní data jako aktivum sui generis cenná nejen pro společnost jako celek, ale také pro jednotlivce, neboť se spolupodílí na vytváření části jejich identity.[74] Jaký způsobem však osobní údaje definuje současná Unijní legislativa?

[74] V této souvislosti lze například zmínit koncept "*informational body*", který lze z anglického originálu doslova přeložit jako informační tělo, hovoří o pomyslném druhém těle fyzické osoby tvořeném digitálními informacemi. Tyto informace mohou být vytvořeny v digitálním světě přímo fyzickou osobou a nebo mohou být derivativního charakteru. Tento pojem zavedl italský filosof Luciano Floridi. Blíže například FLORIDI, Luciano, Carl ÖHMAN *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*

Základním pramen ochrany osobních údajů je nařízení GDPR,[75] jež ve svém článku 4 odstavci 1 definuje osobní údaje jako veškeré údaje, které se vztahují k identifikované či identifikovatelné fyzické osobě - subjektu osobních údajů.

Identifikovanou osobou je subjekt osobních údajů v případě, kdy je součástí zpracovávaných dat určitý přímý identifikátor, za jehož pomoci lze jednoznačně určit konkrétní osobu. Může jím být jméno, identifikační číslo, lokalizační údaje, síťový identifikátor a další. Postačí však i určitý charakteristický rys díky němuž je daná osoba jednoznačně odlišitelná.[76] Jinými slovy, množina osob, které mají přiřazeny konkrétní soubor atributů bude rovna jedné osobě.

Subjektem zpracování osobních údajů je pak pouze fyzická osoba. Což přináší pro datapooling celou řadu nečekaných benefitů. Pravděpodobně nejdůležitějším z nich je pak vyloučení dat právnických osob z okruhu na něž se uplatňují zpřísněná pravidla ochrany osobních údajů. Jestliže tedy jsou v datapoolu sdílena, například data zákazníků, jimiž jsou právnické osoby, sem musí splňovat zpřísněný kritéria ochrany osobních údajů. Další poněkud překvapivou skupinou, na něž se GDPR nevztahuje, jsou zesnulé osoby.[77] U posledně zmíněných však vyvstává otázka, do jaké míry je vzhledem k formální nezávaznosti odůvodnění, toto pravidlo v praxi vynutitelné. Přičemž vyšší míru jistoty nepřináší ani judikatura ESD.[78] Spokojme se proto pro účely této práce s tím, že odkážeme na konkrétní legislativu jednotlivých členských států, která se přes svoje výslovné zmocnění tuto problematiku upravovat, touto problematikou sporadicky zabývá.[79] Má však tato mezera v zákoně na oblast datapoolingu reálný vliv? Jakkoli se to může zdát tento bod poněkud bizarní, nechráněná data

---

[75] Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR)

[76] Například jediný klient, který jezdí na pracovní schůzky společnosti Františkova data s.r.o. na kole, či jediný zvěrolékař ve vsi Horní Zvonková. Osoba může být identifikovatelná i na základě informativní hodnoty údajů jako celku i když každý sám by k identifikaci osoby nevedl.

[77] Odstavec 27 odůvodnění GDPR

78 Blíže například rozsudky v předběžných otázkách C-162/97 Nilsson and others; C-549/07 Wallentin - Herman; C-412/93 Leclerc-Siplec v TF1 and M6

[79] STREJCOVÁ, Adéla, *I am dead, long life to me*: *Digital resurrection of personality in the perspective of European law*, SVOČ, 2023

zesnulých osob jsou potenciálně neocenitelným zdrojem levných cvičných datasetů pro vývojáře a základem celého nového ekonomického odvětví.[80]

Přesuňme se však od definice osobních údajů jako takových k zákonným titulům jejich zpracování. V režimu GDPR existují v zásadě tři nejvýznamnější tituly na základě kterých mohou soukromé datapooly bez vazeb na veřejnou správu, zpracovávat data. A sice zpracování ex lege v rozsahu nezbytně nutném pro plnění smlouvy[81] či pro splnění zákonných povinností[82] na straně jedné a zpracování na základě informovaného souhlasu poskytnutého subjektem osobních údajů[83] na straně druhé. Jakousi zbytkovou kategorií je pak zpracovávání osobních údajů na základě oprávněného zájmu[84] správce osobních údajů. Ostatní tituly zpracování osobních údajů se pak týkají bezprostřední interakce s veřejnou mocí[85] a proto se jimi jak již bylo nastíněno v úvodu nebudeme v této práci zabývat.

Pro datapooling je tedy beze sporu nejvýznamnější zpracování na základě informovaného souhlasu neboť data shromážděná v datapoolu nejčastěji mapují chování zákazníků a to zejména pro účely marketingu a vývoje. Dalším typickým případem zpracování osobních údajů v datapoolu je sběr dat pro výzkum prováděný soukromými výzkumnými institucemi a nebo odděleními pro vědu a výzkum. Ani získáním informovaného souhlasu však zákonné povinnosti pojící se se zpracováním osobních dat v datapoolu nekončí a strany DSA jako správci či zpracovatelé musí splňovat celou řadu kritérií, z nichž některá získávají v prostředí datapoolu specifický význam a proto si je v následujících podkapitolách rozebereme.

3.1 Informovaný souhlas

Jak již bylo zmíněno výše, informovaný souhlas je v drtivé většině případů alfou a omegou zpracování osobních údajů v datapoolu. Proto musí být

---

[80] Viz blíže například Floridi zavádějící koncept Digital Afterlife Industry viz. FLORIDI, Luciano, Carl ÖHMAN. *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry.*, či dále NAKAGAWA, Hiroshi, Akiko ORITA. *Using deceased people's personal data.*

[81] Článek 6 odst. 1 písmeno b) GDPR

[82] Ibid. písmeno c)

[83] Ibid. písmeno a)

[84] Ibid. Písmeno f)

[85] Ibid. písmeno e)

dostatečně široký, tak aby nebránil ekonomicky výhodnému fungování společností jež vystupují v pozici správců osobních údajů, zároveň však musí být dostatečně konkrétní a srozumitelný proto aby subjekt zpracování osobních údajů mohl efektivně chránit svá práva.

Rozeberme si tedy jednotlivé aspekty souhlasu se zpracování m osobních údajů, tak jak jej zakotvuje článek 7 GDPR, v návaznosti na článek 4 odstavec 11 téhož nařízení, definující souhlas jako takový.

3.1.1 Informovanost

Prvním a pravděpodobně nejproblematičtějším aspektem souhlasu je dostatečná informovanost subjektu zpracování osobních údajů o rozsahu a faktického významu zpracování, ke kterému subjekt svůj souhlas propůjčuje. V jakém rozsahu tedy nutné informace poskytnout? Při poskytování souhlasu se zpracováním osobních údajů se nevyhnutelně musí projevit jistá informační asymetrie mezi správcem a subjektem osobních údajů, který souhlas poskytuje. Subjekt osobních údajů jako uživatel patrně nikdy nebude mít stejné množství informací o tom jaké konkrétní operace bude zpracovatel s jeho osobními daty uskutečňovat. Existují pro to dva důvody. Zaprvé, subjekt osobních údajů není dostatečně kompetentní k tomu znát postupy a technologie v oblasti ICT, které jsou ke zpracování jeho dat použity. Zadruhé, udržovat si detailní přehled o konkrétních technikách a přesných místech zpracování je z důvodu množství téměř nemožné a to i s ohledem na to, že jistá část řetězce potřebných informací zpravidla bývá obchodním tajemstvím správce. Jedná se například o zdrojový kód systému atd. Hovoříme-li o množství dat, která datapooly zpracovávají, uveďme pro ilustraci pro datapooling jedno z nejvýznamnějších ekonomických odvětví, a sice společnosti založené na zpracování dat.[86] Tyto společnosti o uživateli zpracovávají asi 52.000 atributů.[87]

Z výše uvedeného je patrné, že subjekt osobních údajů musí v zájmu zachování informovanosti a možnosti svobodně nakládat se svými daty dostat informace ve formě, která pro něj bude snadno přístupná a nebude vyžadovat

---

[86] Zkratka angl. Data-Diven companies více např. VAN DE WAERDT, Peter. Information asymmetries: recognizing the limits of the GDPR on the data-driven market, nebo SCHÄFER, Fabian, Heiko GEBAUER, Christoph GRÖGER, Oliver GASSMANN a Felix WORTMANN. Data-driven business and data privacy: Challenges and measures for product-based companies.

[87] Stanovisko Evropského inspektora ochrany údajů č. 3/2018 o online manipulaci a osobních datech, strana 8. Dostupné z https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf [Citováno 5. února 2024]

neúměrné úsilí.[88] Tuto podmínku splňuje poskytnutí informace o účelu zpracování a totožnosti správce či správců, jejich kontaktní údaje atp.[89] S výjimkou zpracování za pomocí systémů užívající umělou inteligenci a předávání dat do třetích zemí,[90] však subjekt osobních údajů nemusí získat informace o způsobu uložení.

Způsob a rozsah zpracování osobních údajů se v datapoolu může s ohledem vývoj společností velmi dynamicky měnit. Je proto žádoucí aby se strany DSA vyhnuly nutnosti znovuzískávání informovaných souhlasů od subjektů osobních údajů, které jako takové musí proběhnout ještě před plánovanou změnou zpracování a může způsobit takovou časovou ztrátu, která by znamenala stěžejní tržní výhodu pro konkurenci. Navíc požadování nového souhlasu se zpracováním osobních údajů bude mít za následek zmenšení datasetu, jelikož některé subjekty zpracování již znovu souhlas neudělí. Proto je vhodné aby byl zachován účel zpracování osobních údajů v rozsahu ke kterému již dala osoba souhlas. Samotná změna algoritmu, který data zpracovává přitom nehraje roli, i přesto, že může vést k získání zcela jiného okruhu derivativních informací. Původní souhlas je v takovéto případě platný, pokud je stále zpracováván původní rozsah primárních dat a je zachován účel samotného zpracování. Zjednodušeně řečeno tedy nemá kvalitativní efekt využívání dat na platnost souhlasu vliv.

Další obligatorní součástí souhlasu jsou informace o osobě správce osobních údajů ale rovněž o tom, kterým třetím stranám jsou data poskytována. V okamžiku získání souhlasu však nemusí být zcela jasná identita všech stran sdílející budoucí datapool, proto postačí určení samotné kategorie příjemců. Správce osobních údajů však musí být v tomto ohledu připraven na možnost subjektu zpracování osobních údajů se jmenovitě dotázat na to jakým entitám jsou

---

[88] Subjektu údajů musí být v souladu s článkem 12 odst. 1 GDPR poskytnuta informace "… *stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků…*"

[89] Výčet obsahují zejména články 13 a 14 GDPR. Taxativní výčet informací, které musí správce údajů poskytnout však nalezneme ve článku 12 GDPR

[90] Článek 13 odst. f) GDPR

jeho data zpřístupněna a v takovém případě poskytnut dostatečné identifikační údaje všech entit, které se v daném okamžiku na datapoolu podílejí.[91]

Z tohoto důvodu je v některých případech v zájmu zachování obchodního tajemství týkajícího se spoluprací společností funkčně rozdělit datapool, který je přístupný více společnostem do sekcí tak, aby osobní data klientů byla v sekci ke které mají přístup pouze společnosti, které je reálně potřebují a nedocházelo tak ke zbytečnému odhalování dalších obchodních partnerů.

V neposlední řadě pak nelze poskytnout souhlas ke zpracování dat způsobem, který je ex lege zakázán. Takovýmto souhlasem pak bude zejména souhlas uživatele, který je mladší 16ti let.[92] Za rozporný s právními předpisy pak může být rovněž požadován souhlas, který nemůže subjekt osobních údajů efektivně odmítnout poskytnout ať už díky designu rozhraní, ke kterému přistupuje, či kvůli tomu, že na poskytnutí souhlasu je vázán přístup k určitému zboží a nebo službě za předpokladu, že samotné plnění smlouvy tyto výsledky nevyžaduje.[93]

3.1.2 Forma souhlasu

Pravděpodobně nejdůležitějším aspektem informovaného souhlasu z pohledu kontroly dodržovaní informační povinnosti správce vůči subjektu zpracovávaných osobních údajů je jeho písemná forma.[94] Požadavek písemné formy přitom splňuje i písemné prohlášení, které je učiněno elektronicky, například zaškrtnutími políčka.[95] V oblasti poskytnutí osobních údajů má však tato písemná forma jistá specifika. Předně potřeba jednoznačně a zřetelně odlišit

---

[91] Viz. například body 48 a 51 rozsudku ve věci C-154/21 Österreichische Post. Zde Soudní dvůr Evropské unie dovodil, že "*…za určitých okolností není možné poskytnout informace o konkrétních příjemcích. Právo na přístup tedy může být omezeno na informace o kategoriích příjemců, není-li možné sdělit totožnost konkrétních příjemců, zejména pokud ještě nejsou známi*." Zároveň však dodává, že "*…že právo subjektu údajů na přístup k osobním údajům, které se ho týkají, stanovené tímto ustanovením, znamená v případě, že tyto údaje byly nebo budou zpřístupněny příjemcům, povinnost správce sdělit tomuto subjektu totožnost těchto příjemců, ledaže je nemožné identifikovat tyto příjemce nebo uvedený správce doloží, že žádosti subjektu údajů o přístup jsou zjevně nedůvodné nebo nepřiměřené ve smyslu čl. 12 odst. 5 GDPR, v kterýchžto případech může správce poskytnout subjektu údajů informace pouze o kategoriích dotčených příjemců.*"

[92] Jednotlivé členské státy mohou tuto hranici právním předpisem v souladu s článkem 8 odst. 4 GDPR snížit až na 13 let. Tento souhlas lze v určitých situacích nahradit souhlase zákonného zástupce a nebo osobní data těchto subjektů zpracovávat na základě jiného právního důvodu.

[93] Odstavec 43 odůvodnění GDPR

[94] Článek 7 odst. 2 GDPR

[95] Odstavec 32 odůvodnění GDPR

souhlas se zpracováním osobních údajů od dalšího obsahu tak, aby bylo bylo prokazatelné, že si je subjekt osobních údajů vědom, že souhlas poskytuje.[96]

GDPR tak vzhledem k citlivosti dat a nevyváženosti pozic mezi subjektem osobních údajů a správcem požaduje i odpovídající faktické odlišení tak, aby bylo zjevné, že se skutečně jedná o souhlas se zpracováním. Tento požadavek pak zejména reaguje na faktickou potřebu takového jednání zejména u komplexnějších smluv, ve kterých bylo běžnou praxí, ustanovení o souhlasu se zpracováním osobních údajů skrývat mezi ostatní text.[97]

Praktický výkon tohoto pravidla pak není nikterak složitý. Za dostatečnou formu odlišení lze považovat vytučnění odstavce, jeho orámování, barevné zvýraznění a nebo poskytnutí souhlasu v rámci separátního dokumentu. Posledně jmenovaná varianta je pak obzvláště vhodná z důvodu oddělitelnosti poskytnutí souhlasu se zpracováním osobních údajů od zbytku smlouvy a tím i materiálního poskytnutí plnění v rámci businessových aktivit strany DSA a jejích aktivit spočívajících v získávání cenných dat mj. pro účely sdílení v datapoolu. Z relativně nových nástrojů, které lze k splnění tohoto pravidla použít, je vhodné zmínit tzv. smart contract.[98] I tyto smlouvy však musí být bez výjimečně navrženy tak, aby na jejich základě mohl správce osobních údajů kdykoliv prokázat existenci souhlasu.

3.1.3 Stažení souhlasu

Informovaný souhlas se zpracováním osobních údajů však může subjekt osobních údajů kdykoliv odvolat. V takovém případě musí správce identifikovaná, či identifikovatelná data týkající se tohoto subjektu bezodkladně vymazat.[99] Pro tento účel musí mít jednotliví správci osobních údajů dostatečnou kontrolu nad

---

[96] Vzhledem k tomu, že subjekt osobních údajů bude v drtivé většině případů ve vztahu ke společnosti a nebo společnostem podílejících se na datapoolu spotřebitelem, aplikuje se článek 5 Směrnice Rady 93/13/EHS ze dne 5. dubna 1993 o nepřiměřených podmínkách ve spotřebitelských smlouvách, v ostatních případech se toto ustanovení použije analogicky ve vazbě na nerovný vztah.

[97] KOSTA, Eleni in KUNER, Christopher; BYGRAVE, Lee; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU General Data Protection Regulation (GDPR); A Commentary*. Oxford University Press, 2020. ISBN 978–0–19–882649–1. Strana 350.

[98] Do češtiny poněkud neobratně překládáno jako *chytrá smlouva*, slovy Nicka Szabo se jedná o "*...počítačový transakční protokol, který provádí podmínky smlouvy. Obecnými cíli návrhu chytrých smluv je splnit běžné smluvní podmínky (jako jsou platební podmínky, zástavní práva, důvěrnost a dokonce i vymáhání)....*" SZABO, Nick. *Smart Contracts*. Online. Dostupné z: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. [Citováno 22. března 2024]

[99] Odstavec 1 a odstavec 1 písm b) článku 17 GDPR

obsahem datapoolu, tak aby bylo možné rychlé a efektivní splnění této povinnosti. Tato kontrola spočívá zejména v přístupových právech do systému datapoolu, která zahrnují oprávnění mazat data. Dalším velmi vhodným technickým opatřením je programové vybavení datapoolu, které svým navržením umožňuje efektivní a co nejjednodušší vyhledání dat, která mají být smazána a samozřejmě jejich smazání a to buď manuálně a nebo k tomu určeným promptem. Stažení souhlasu se zpracováním osobních údajů jako projev vůle je možné konat vůči kterémukoliv ze společných správců a to jak správců sdružených v datapoolu tak i případných správců mino něj, pokud byl souhlas poskytnut společně pro více druhů zpracování. Tento fakt pak přímo implikuje možnost subjektu osobních údajů stáhnout souhlas pouze pro určitou separátní činnost v rámci zpracování jeho osobních údajů a nebo pouze pro určitého ze správců. Aby se orginární správce, který původně fyzicky získal souhlas jakožto dokument, ve kterém subjekt souhlasí se zpracováváním svých údajů i správci v datapoolu vyhl nutnosti smazat data i ze svých databázích v případě ztráty důvěry subjektu v bezpečnost datapoolu, je vhodné poskytovaný souhlas rozdělit tak, aby následně bylo možné stáhnout pouze jeho část dovolující sdílení dat s dalšími správci a nebo zpracovateli datapoolu, případně souhlas rozdělit již na začátku do dvou dokumentů.

Stažení souhlasu se přitom netýká pouze vložených dat, ale i metadat a identifikovatelných derivativních dat. Na tuto povinnost je proto nutné myslet již při návrhu softwarového řešení, které bude pro datapool zvoleno. I zde se mimořádně vyplatí, pokud je informovaný souhlas koncipován jako *smart contract*, jelikož v tomto případě, je možné na stažení souhlasu přímo k tomu určený algoritmus, který automaticky v řádu sekund požadavek provede.[100] Tato rychlost společně se zpětnou notifikací o tom, že byl požadavek proveden pak přispívá nejen k upevnění právní jistoty subjektu osobních údajů ale i k zachování případných dobrých obchodních vztahů s původními správci jakožto společnostmi.

---

[100] Ne všechny formy smart contract jsou pro udělení souhlasu se zpracováním osobních údajů vhodné. Některé koncepty užívající dencentralizovaná nepřepisovatelná úložiště jako je například IPFS (zkratka z angl. Interplanetary File Storrage) jsou z hlediska nemožnosti výmazu byť šifrovaných údajů, zcela nevhodné. Blíže k na vrhovanému systému IPFS WANG, Shangping, Yinglong ZHANG, Yaling ZHANG. *A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems*. IEEE Xplore, vol. 6, z roku 2018. ISSN: 2169-3536 pp. 38437-38450. Dostupné z: http://dx.doi.org/10.1109/ACCESS.2018.2851611

3.1.4 Svobodný projev vůle subjektu

Posledním ze čtveřice nejvýznamnějších aspektů souhlasu se zpracováním údajů je aspekt svobodného projevení vůle.[101] Přesto, že je ve srovnání s předchozími odstavci článku 7 GDPR tento pravděpodobně nejvíce opomíjen, je v něm obsažené pravidlo, pomyslnou korunou která celý koncept informovaného souhlasu zastřešuje a bez níž by ostatní aspekty jednoduše postrádaly význam. I sebelepší informovanost subjektu osobních údajů, zachycená ve formálně perfektním formuláři doplněném o poučení o možnosti souhlas odvolat, jednoduše ztrácí smysl, pokud je tento dokument odsouhlasen v důsledku (byť i nepřímého) vynucení.

Souhlas se zpracováním osobních údajů by tak neměl mít kontraktační charakter v tom smyslu, že subjekt osobních údajů vymění svoje soukromí za možnost uzavření smlouvy na plnění, které s poskytovanými údaji vůbec nesouvisí a nebo v rozsahu, který není nezbytný.

Pracovní skupina WP 29 (dnes EDPB) tak ve svých pokynech výslovně uvádí: "*…cílem právních předpisů na ochranu údajů je ochrana základních práv, je kontrola jednotlivce nad jeho osobními údaji zásadní a existuje silný předpoklad, že souhlas se zpracováním osobních údajů, které není nezbytné, nelze považovat za povinnou protihodnotu výměnou za plnění smlouvy nebo poskytnutí služby*."[102] Určit přesnou hranici, které údaje jsou samy o sobě k plnění smlouvy potřeba je přitom delikátní problém a za účelem zachování jistoty zákonnosti zpracování by měl být výklad meze dobrovolnosti souhlasu spíše restriktivní.

V této souvislosti je vhodné zmínit, že existují skupiny osob, které ve vztahu k určitým osobám z povahy nerovnováhy právního ale i faktického vztahu ke správci svůj souhlas efektivně poskytnout nemohou. Jedná se například o zaměstnance poskytující informovaný souhlas zaměstnavateli. Přičemž nelze očekávat, že by zaměstnanec a nebo dokonce i uchazeč o zaměstnání mohl takovýto souhlas odepřít bez toho aby se obával negativních následků pro jeho osobu. Jakkoli by tedy pro strany datapoolu byla lákavá možnost sdílení dat například o dostupných uchazečích na trhu práce v daném oboru, například za

---

[101] Článek 7 odst. 4 GDPR

[102] Pokyny pro souhlas podle nařízení 2016/679 přijaté dne 28. listopadu 2017 v revidovaném znění přijatém dne 10. dubna 2018 Pracovní skupinou zřízenou podle článku 29. Online. Strana 8. Dostupné z: https://www.ipvz.cz/seznam-souboru/4864-pokyny-pro-souhlas-podle-narizeni-vystaveno-dne-14-03-19.pdf [Citováno 30. března 2024]

pomoci některé z forem sofistikovaných ATS, nebude takovéto zpracování ve většině případů jednoduše možné.[103]

Výše zmíněný příklad vztahů nerovnováhy mezi subjektem osobních údajů a správcem či správci však v žádném případě není jediný, ba právě naopak. Prostředí moderních datapoolů bude nekonečným zdrojem takovýchto situací. Směrodatnou otázkou pro svobodu poskytovaného souhlasu, kterou si musí správce při sestavování textu souhlasu se zpracováním osobních údajů musí položit, je zda subjekt může bez podstatných negativních následků poskytnutí souhlasu odmítnout a zda je mu absence takovéhoto rizika zjevná nebo zda je naopak v určité pozici rozumné se takovéhoto rizika obávat.[104]

3.2 Postavení správce a zpracovatele osobních údajů

Vzhledem k variabilitě možností a struktur právních vztahů, které mohou společnosti mezi sebou v rámci DSA ujednat, je téměř nemožné obecně stanovit formu, vztahu, který budou mít jednotlivé společnosti ve vztahu k osobním údajům. Lze však definovat určitá vodítka, v závislosti na nichž bude každý jednotlivý datapool koncipovat ochranu osobních údajů. V první řadě je potřeba určit, zda se jedná o dataopool s vertikální a nebo horizontální organizační strukturou.[105] Zda jsou osobní data získávána prostřednictvím jednotlivých stran DSA a nebo zda jsou získávána přímo datapoolem od samotných uživatelů. [106] Dalším hlediskem je, zda mají strany datapoolu přístup přímo k osobním údajům a nebo zda jsou do datapoolu nahraná data obratem anonymizována a vytěžena

[103] Toto akcentuje i článek 88 GDPR, který výslovně zmocňuje jednotlivé členské státy k přijetí národní úpravy, která vzhledem k lokálním poměrům konkretizuje rozsah osobních údajů, které může zaměstnavatel legálně zpracovávat.

[104] Například i když by konkrétní zaměstnavatel neposkytnutí souhlasu s extensivním zpracováním osobních údajů nijak nesankcionoval, zaměstnanec má rozumný důvod se takovéhoto jednání obávat a proto zaměstnavatel vůbec nesmí souhlas se zpracováním v této věci vůbec požadovat.

[105] Toto rozlišení je důležité z hlediska rozhodovacích práv stran a tím pádem i determinaci, v jakém rozsahu budou strany správci a nebo zpracovateli.

[106] Byť se jedná o jev spíše okrajový, některé datapooly mohou mít vlastní právní subjektivitu a proto by v případě přímého získávání dat od subjektů osobních údajů mohly vystupovat jako správci pouze ony datapooly a nikoli strany, které datapool založily. To však za předpokladu, že by tyto strany obdařily datapool jako právnickou osobu vlastními rozhodovacími pravomocemi ve vztahu k rozsahu a způsobu zpracování dat, přičemž účel zpracování dat by byl vymezen v zakladatelské listině datapoolu jako právnické osoby. Současně by musela být splněna podmínka limitu faktického podílu jednotlivých společností na fungování datapoolu jako separátní společnosti, tak aby byla dostatečně diverzifikována. Ergo žádná ze společností by nesměla mít ve vztahu k datapoolu postavení ovládající společnosti.

tak, že další strany mají přístup pouze k výsledku výpočetního procesu a nikoli k jednotlivým identifikovatelným datům.[107]

Teprve pokud pokud jsou důkladně posouzena všechna výše zmíněná kritéria, je možné s jistotou určit otázku, které z fyzických a právnických osob podílejících se na datapoolu jsou správci, které jsou zpracovateli a které z osob nemají k osobním údajům žádný právní vztah. Tato statusová otázka pak zásadním způsobem determinuje rozsah práv a povinností, kterými jednotlivé strany disponují viz. níže.

Než se však zplna ponoříme do rozebírání jednotlivých nuancí postavení jednotlivých entit vytvářející datapool, zaměřme se aspoň v rychlosti na vymezení jednotlivých základních statusů ve vztahu ke zpracovávání osobních údajů. Začněme nejprve se správcem. Správce, osobních údajů je osoba, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.[108] Správcem tedy bude pro účely datapoolu osoba, která data získala od subjektů osobních údajů ale i další osoby, kterým bude poskytnuto v informovaném souhlasu právo s osobními údaji nakládat. Což v praxi znamená, že se správcem mohou stát i ostatní společnosti v datapoolu, za předpokladu, že s tím byl subjekt zpracování osobních údajů dostatečně jasně srozuměn při poskytnutí informovaného souhlasu. Postavení správců osobních údajů se však mohou ostatní subjekty sdružené v datapoolu zprostit, jestliže dojde k anonymizaci dat, ještě před jejich nahráním do datapoolu. Tento postup lze proto v maximální míře doporučit, neboť se tak strany datapoolu vyhnou rizikům spojených s únikem takovýchto údajů. Dalším takovým benefitem je, že se datapool vyhne zkreslení určité části datasetu v případě, kdy by byl požadován některými subjekty osobních údajů výmaz jejich osobních dat.[109]

Zpracovatele osobních údajů je naproti tomu osoba, která na základě pokynů správce provádí uložení a nebo jiné zpracování osobních údajů. Tato osoba podléhá stejným standardům ochrany osobních údajů, ovšem s tou výjimkou, že nerozhoduje o účelu ani způsobu zpracování osobních údajů a pouze plní pokyny správce. Zpracovateli tak mohou ve vztahu k datům uloženým v

---

[107] V takovém případě, by byl správcem pouze přispěvatel a ostatní strany by byly v závislosti na konkrétním zvoleném technickém řešení pouze zpracovateli a nebo by k osobním datům neměly dokonce žádný vztah.

[108] Článek 4 odstavec 7 GDPR

[109] Blíže v kapitole Výmaz osobních údajů

datapoolu být zejména společnosti, které pro něj zajišťují cloudové služby ve smyslu PaaS a SaaS. Což ovšem neznamená, že by se poskytovatelé cloudových služeb SaaS nemohli stát za rovněž správci osobních údajů a to z toho titulu, kdy budou určovat způsob zpracování těchto údajů a to například formou zákazníkům přímo na míru navržených technik zpracování o jejichž struktuře rozhodují.[110]

V případě, že se strany datapoolu dohodnou, že vložená data do datapoolu nebudou anonymizovat, pak bude mezi jednotlivými společnostmi tvořícími datapool vůči subjektům osobních údajů vznikat vztah společných správců a to i v případě, že nebudou obsahově mít k osobním údajům plný přístup.[111]

Pro pochopení konceptu společných správců je vhodný alespoň krátký historický exkurs. Současný koncept se totiž inspiroval britskou úpravou obsaženou v paragrafu 1 odstavce 1 zákona Spojeného království o ochraně dat z roku 1998.[112] Tento zákon v podstatě předpokládal koexistenci dvou zpracovatelů, kteří těží z jednoho zdroje dat. Přičemž správce byl osobou, která společně s ostatními určovala jaká data a jakým způsobem budou zpracovávána. Společní správci dat byli rovněž povinni mezi sebou uzavřít kontrakt, který měl za úkol zajistit, že budou dodrženy podmínky pro zpracování dat.[113] V praxi tak šlo o úpravu, která byla na míru tvořená předchůdcům datapoolů tak, jak je známe dnes.

Dnešní evropská úprava společných správců osobních údajů podobně jako její britská předchůdkyně určuje povinnost společných správců mezi sebou transparentně ujednat způsob zpracování a určit podíl a role při odpovědnosti, které jednotlivé společnosti za zpracování osobních údajů v rámci datapoolu ponesou a to zejména ve souvislosti s dozorem příslušných úřadů.[114] Nejčastěji bude přitom převažovat zodpovědnost jednotlivých společností za určité vybrané operace v rámci zpracovávání dat. Například za zpracování dat až do fáze jejich

---

[110] Například bod. 38 rozsudku v předběžné otázce ve věci Wirtschaftsakademie Schleswig-Holstein, C-210/16

[111] Článek 26 GDPR

[112] Dostupný například z https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted

[113] MILLARD, Christopher, Dmitra KAMARINOU in KUNER, Christopher; BYGRAVE, Lee; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU General Data Protection Regulation (GDPR); A Commentary*. Oxford University Press, 2020. ISBN 978–0–19–882649–1. Strana 584.

[114] Recitál GDPR odstavec 79

nahrání na společné úložiště jako je čištění a kategorizace, ponese obvykle zodpovědnost společnost, která je prvotně shromáždila od jednotlivých uživatelů. Naproti tomu, za pochody v datapoolu bude zodpovědnost rozdělena mezi jednotlivými stranami DSA[115] sdílená v takové míře v jaké při zpracování dat navrhují a zajišťují jednotlivé technologické a administrativní procesy.[116]

Jedním ze stěžejních aspektů dohody společných správců je zejména ujednání, v jakém rozsahu se budou podílet jednotlivé společnosti na zajištění určitých práv subjektu osobních údajů jako je právo na výmaz, právo na poskytnutí informace o druhu a množství zpracovávaných dat ve vztahu ke konkrétnímu subjektu a také odpovědnost za správnost zpracovávaných údajů. Dalším důležitým okruhem povinností je přitom i odpovědnost za přijetí odpovídajících opatření v oblasti kyberbezpečnosti, hlášení úniků osobních dat a zpracování posouzení vlivu na ochranu osobních údajů DPIA. Kvalitní a jasné rozdělení je důležité i z pohledu zamezení negativního konfliktu mezi jednotlivými správci, díky kterému by mohla (často i nevědomky) vznikat při zpracovávání údajů nechráněná místa, která by se stala snadným cílem pro zneužití.[117] Při efektivním rozdělení rozdělení rolí jednotlivých správců osobních údajů je zásadní brát v potaz možnosti a kvalifikaci jednotlivých správců ve vztahu k jim přiděleným rolím. Vaše uvedené má zajistit konečné efektivní splnění povinností vyplývajících z GDPR a dalších předpisů jednotlivých členských států ve vztahu ke zpracování osobních údajů za které jsou správci odpovědní společně. Pro tento účel stanovení efektivního nastavení poměrů je pak vhodná za tím účelem provedená interní analýza. V zásadě lze totiž říci, že v souladu s principem smluvní volnosti si mohou strany DSA sjednat v podstatě jakékoliv rozdělení a míru zatížení různých stran povinnostmi, přičemž rozdělení povinnosti ve vztahu k zajištění ochrany dat nemusí být vůbec rovnoměrné. Jediným požadavkem na takováto ujednání v rámci DSA je potom konečné

---

[115] Za předpokladu, že bude ujednání dostatečně transparentní, je možné aby si strany datapoolu ujednaly rozsah míru svého zapojení i mimo DSA a to třeba i formou právně nezávazného dokumentu. (Strana 4 Pokyny pro souhlas podle nařízení 2016/679 přijaté dne 28. listopadu 2017 v revidovaném znění přijatém dne 10. dubna 2018 Pracovní skupinou zřízenou podle článku 29) Tento postup však nelze doporučit z mnoha důvodů. Předně závazky vyplývající z právně nezávazného dokumentu jsou výrazně hůře vymahatelné. Dále pak separátní dokument, byť i právně závazný poskytuje prostor pro administrativní chybu ve vztahu k měnícímu se okruhu společností tvořících datapool.

[116] Blíže odstavec 163 Pokyny pro souhlas podle nařízení 2016/679 přijaté dne 28. listopadu 2017 v revidovaném znění přijatém dne 10. dubna 2018 Pracovní skupinou zřízenou podle článku 29.

[117] Ibid. odstavec 160.

splnění všech povinností a dosažení požadované úrovně ochrany osobních údajů.[118]

Rozsah a způsob zpracování se pak může velmi dynamicky měnit. Vždy ovšem v rozsahu ve kterém si společnosti od subjektů osobních údajů opatřily informovaný souhlas. Pokud se v rámci takových změn dostane do rozporu faktický stav se stavem ujednaným v původním DSA, převáží faktický stav. Tato situace je ovšem vysoce nežádoucí a to jak z pohledu těch stran, které původně určitou operaci vykonávaly a formálně za ni stále nesou odpovědnost. Tak z důvodu snížené transparentnosti zpracování, za kterou mohou být členové datapoolu postihováni. Tato dílčí smluvní odpovědnost působí v případě porušení spíše jako nástroj pro případné vymáhání náhrady škody a dalších občansko právních nároků mezi jednotlivými stranami DSA a jako vodítko pro autority, kontrolující dodržování pravidel ochrany osobních údajů, nemá však vliv na odpovědnost za zajištění zákonnosti zpracování a souladu zpracování se základními principy zpracování osobních údajů.[119]

Nehledě na rozdělení funkcí tak nese každý ze správců osobních údajů odpovědnost za zpracování osobních údajů a to v tom rozsahu, že jím získaná data ostatní správci zpracovávají v souladu s původním účelem a v rozsahu, ke kterému byl poskytnut informovaný souhlas.[120] Naproti tomu pak stojí povinnost ostatních správců ujistit se, že zpracovávají osobní údaje způsobem a v rozsahu, který informovaný souhlas získaný jiným správcem dovoluje. V souladu s výše zmíněným je jaksi imanentní povinnost každého ze správců ujistit se že takovýto souhlas vůbec existuje.

Tento komplikovaný koncept rozdělení sdílené odpovědnosti mezi společnými správci osobních údajů pak pouze dokresluje fakt, že subjekt osobních údajů může uplatňovat svá práva v souvislosti se zpracováním osobních údajů vůči kterémukoliv ze společných správců osobních údajů,[121] bez ohledu na to který z nich od něj v prvopočátku získal informovaný souhlas se zpracováním. Subjekt osobních údajů by měl být přitom informován o podstatných prvcích

---

[118] Odstavec 165 Pokynům 07/2020 k pojmům správce a zpracovatele v GDPR Verze 2.0 přijaté dne 7. července 2021 přijaté EDPB

[119] Ve smyslu článku 5 GDPR

[120] Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR Verze 2.0 přijaté dne 7. července 2021 přijaté EDPB, strana 4

[121] GDPR článek 26 odst. 3

ujednání o rozdělení rolí při zpracování osobních údajů mezi jednotlivými správci[122] tak aby mohl efektivně chránit svá práva. Informace o rozvržení povinností mezi správci osobních údajů takmůže představovat zásadní faktor při rozhodování zda souhlas udělit a to v souvislosti s tím jak subjekt osobních údajů vnímá důvěryhodnost jednotlivých společností.

3.3 Minimalizace zpracování osobních údajů

Vzhledem ke zvýšené míře citlivosti osobních údajů ve srovnání s ostatními skupinami dat a rozsahu potřebných opatření k zajištění jejich bezpečného zpracování v souladu s legislativou, je bezpochyby vhodné si nejdříve zodpovědět otázku, jaký je primární účel data poolu a zda je potřeba aby v něm osobní údaje byly vůbec sdíleny. Pokud by totiž šlo účelu, který je dosahován za pomoci zpracovávání osobních údajů docílit i tím, že by byla zpracovávána například anonymizovaná data uživatelů, je beze vší pochybnosti nejvhodnějším řešením toto tento modus fungování použít, v souladu s principem minimalizace[123] zpracování osobních údajů, toto řešení.

Tento princip se pak rovněž uplatní v úvahách o rozsahu zpracovávaných osobních údajů. I když je toto maximum v podstatě v přímém rozporu se světem tzv. *big data*, který jak už anglický název napovídá, usiluje o práci s velkým množstvím dat, ze kterého se snaží vytěžit co nejkvalitnější informace a jehož je datapooling zpravidla klasickým příkladem, lze zde najít přeci jenom určitá východiska. Zaprvé množství osobních údajů zpracovávaných v datapoolu vůbec nemusí být jako takové malé, musí však být nejmenší nezbytně nutné k tomu, aby byl rozumným způsobem splněn daný účel, ke kterému jsou zpracovávána. Toto množství samozřejmě často není jednoznačně definovatelné. Jako určité vodítko slouží jeho negativní vymezení a sice fakt, že nesmí být zpracovávány osobní údaje, které jsou pro daný účel zbytečné. Princip minimalizace zpracování se dále projeví v časovém horizontu v jakém jsou data zpracovávána, touto problematikou se budeme zabývat v následující kapitole.

3.3.1 Plán výmazu osobních údajů

Součástí každého legálního a ekonomicky udržitelného zpracování osobních údajů musí být krom jejich získávání i plán jejich odstraňování. Přičemž

---

[122] Článek 26 odst. 2 GDPR

[123] Článek 5 odstavec 1 písmeno c) GDPR a jemu odpovídající odstavec 39 odůvodnění

o tom, jak dlouho budou jeho data zpracovávána, musí dostat subjekt osobních údajů alespoň rámcovou informaci již na samém počátku při udílení souhlasu. V případě zpracovávání osobní dat ex lege je pak délka zpracování omezena na dobu nezbytně dlouhou pro splnění zákonné povinnosti.[124] Výše zmíněné tak odráží dvě stěžejní zásady obsažené ve článku 5 odstavci 1 GDPR zásadou *omezení uložení* společně s výše rozebranou zásadou minimalizace.[125] V kontextu datapoolů bude rozhodujícím faktorem pro výmaz konkrétních osobních dat zejména jejich cirkulace. A sice z jak velkého a stabilního reprezentativního vzorku dat datapool čerpá.

V praxi tak bude zapotřebí mnohem kratšího skladování osobních dat při marketingovém průzkumu, který má za cíl prodat zboží z letní kolekce konkrétně identifikovaným zákazníkům, kteří již zakoupili zimní kolekci, než v případě longitudiálního vědeckého výzkumu stárnutí jednovaječných dvojčat. U zákazníků totiž velmi záhy přestanou být konkrétní osobní údaje potřeba (v okamžiku ukončení prodeje letní kolekce). A bude možné buď množství dat omezit na naprosté minimum (například informace, zda zákazník preferuje tulipány a nebo chudobky již bude irelevantní) a ponechat v databázi pouze základní údaje (emailovou adresu a popřípadě jméno) a nebo je zcela vymazat v případě, že se změní okruh cílových zákazníků (například koncern se rozhodne uzavřít prodejny v Polsku a vymaže data o polských zákaznících). Zatímco u dlouhodobého vědeckého výzkumu bude důležité shromažďovat data po co nejdelší dobu.

Výše zmíněné by pak měl akcentovat plán výmazu osobních údajů přesným určením momentu, kdy jsou již data nepotřebná a je nutné aby byla smazána. Obsah tohoto plánu výmazu pak musí být alespoň ve svých hrubých rysech znám subjektu osobních údajů v okamžiku poskytování informovaného souhlasu se zpracováním osobních údajů. Plné znění plánu výmazu osobních údajů pak musí být natolik konkrétní a průkazné, aby při předložení kontrolnímu úřadu rozptylovalo pochybnosti ohledně zákonnosti zpracování osobních údajů.

3.3.2 Právo na výmaz osobních údajů

Právo subjektu osobních údajů na výmaz jako takové je zastřešujícím ustanovením, které zakotvuje povinnost odstranění osobních dat v případě, že již

---

[124] Článek 6 odst. 1 písmeno c) GDPR

[125] Článek 5 odstavec 1 písm. e) Ibid.

zpracovávané údaje nejsou potřeba,[126] stažení souhlasu se zpracováním osobních údajů,[127] osobní údaje byly zpracovávány protiprávně,[128] osobní údaje musí být vymazány ke splnění právní povinnosti, stanovené v právu Unie nebo členského státu, které se na správce vztahuje[129] a nebo v případě kdy byly osobní údaje shromážděny v souvislosti s nabídkou služeb informační společnosti na základě čl. 8 odst.1[130]. Posledním poněkud složitějším případem povinného odstranění zpracovávaných údajů ze systému správců sdružených v datapoolu je výmaz na základě námitek podle článku 21 GDPR, které mohou být v kontextu datapoolu podány za situace, kdy jsou data zpracovávána jako nezbytná pro účely oprávněného zájmu správce a nebo třetí strany.

V případě, že tedy na základě, kteréhokoli z výše zmíněných důvodů dojde k aktivaci práva na výmaz. Je datapool povinen bez zbytečného odkladu přistoupit k odstranění dat ze svých systémů a to v souladu s rozvržením rolí, které si jednotliví správci ujednali z pozice společných správců v DSA. Vzhledem k tomu, že s výjimkou nepotřebných údajů je právo na výmaz aplikováno na základě právních událostí, které strany datapoolu nemohou uspokojivě předvídat, přináší aplikace článku 17 GDPR celu řadu zcela technologicky právních specifik.

První a pro společnosti přispívající do datapoolu pravděpodobně nejsložitější význvou, je nutnost přizpůsobení architektury datapoolu[131] tak, aby bylo možné identifikovatelná data jednotlivých uživatelů efektivně vymazat a zároveň aby byla co nejméně poškozena kvalita a nedocházelo ke zkreslení výsledků. Takovéto zkreslení výsledků by bylo nejen popřením samotného účelu datapoolu jako platformy v rámci které společnosti sdílejí data ze kterých mohou vzájemně benefitovat, ale v některých případech i práva na přesnost zpracovávaných údajů dalších subjektů osobních údajů[132].

V zásadě jde o to, že při poskytování souhlasu se zpracování osobních údajů a jeho následném stahování a částečně i podávání námitek proti zpracování

---

[126] GDPR čl. 17 odstavec 1 písmeno a)

[127] Ibid. Písmeno b)

[128] Ibid písmeno d)

[129] Ibid písmeno e)

[130] Ibid. odstavec f) odkazující na článek 8 odst. 1 GDPR, který se zabývá okolnostmi poskytnutí informovaného souhlasu dítětem.

[131] V souladu s články 24 a 25 GDPR

[132] Právo na přesnost osobních údajů je zachyceno zejména v článku 5 odst. 1 písmeno d) GDPR

osobních údajů na základě oprávněného zájmu, jsou subjekty osobních údajů jakožto lidé motivovány různými pohnutkami.

Zatímco souhlas se zpracováním osobních údajů podává víceméně různorodá a zpravidla velmi široce definovaná skupina uživatelů informačních technologií, která takovéto jednání činí z celého spektra právních důvodů. Přičemž takovouto pohnutkou může být i tak jednoduchá pudy poháněná touha, jako je rychlé odstranění lišty na displayi zařízení na které se žádost zpravidla nachází, a tím zajištěné lepšího výhledu pro lov, kterým je v kontextu moderní doby nákup zboží. Právo na výmaz však budou spíše uplatňovat skupiny s určitými předpoklady jako je konkrétní skupina obyvatel ke které subjekt náleží.[133] Hlavním faktorem zkreslujícím dataset při výmazu však stále zůstává jejich množství to bez ohledu na zvolenou techniku výmazu dat. Přičemž zhoršování kvality datasetu není lineární proces ale dosahované hodnoty oscilují spíše okolo pomyslné progresivně klesající funkce.[134]

3.4 Posouzení vlivu na ochranu osobních údajů

Dále bude při datapoolingu pro zajištění zákonných podmínek zpracování osobních údajů ve většině případů vyžadováno takzvané DPIA[135], které musí zpracovat společnosti společného datapoolu osobní údaje, jejichž jsou správci. Samotná povinnost zpracování DPIA jakožto posouzení rizik před zahájením zpracovávání údajů určitým způsobem je zakotvena v článku 35 GDPR, má však rovněž oporu v článku 10 odstavci 2 modernizované Úmluvy 108+[136], vydané Radou Evropy.

Článek 10 výslovně stanoví že "*správci a případně zpracovatelé před zahájením zpracování údajů prověří pravděpodobný dopad zamýšleného zpracování údajů na práva a základní svobody subjektů údajů a navrhnou zpracování údajů tak, aby se zabránilo riziku zásahu do těchto práv a základních svobod nebo aby se toto riziko minimalizovalo*."

---

[133] Autorka v tomto směru zcela souhlasí s vyslovenou hypotézou autorského kolektivu Dam, Henzl, Klausen z Institute of IT Security Research St. Pölten, byť se následně v rámci zmiňované práce hypotéza z důvodu nedostatku vhodných zdrojových dat neprokázala a byla k ponechána k prokázání dalším dosud neprovedeným výzkumem. Viz. DAM, Tobias, Maxmilian HENZL, Lukas Daniel KLAUSNER, *Delete My Account: Impact of Data Deletion on Machine Learning Classifiers.* Online. ArXiv 2023. Dostupné z: https://doi.org/10.48550/arXiv.2311.10385

[134] Ibid .

[135] Z angl. Data Protection Impact Assessment

[136] Modernizovaná Úmluva 108+

Narozdíl od GDPR však důvodová zpráva Modernizované Úmluvy 108+ stanoví, že toto ex ante prověření má být prováděno bez dalších přílišných formalit. Tato rozdílnost pak pramení patrně jednak z předchozí datace Úmluvy ve vztahu k Nařízení a jednak z funkčního aparátu institucí a institutů práva, které má Evropská Unie narozdíl od Rady Evropy k tomuto účelu k dispozici.

Modernizovaná Úmluva 108+ je však naopak přísnější v četnosti situací kdy má být takové posouzení risk prováděno, neboť nepodmiňuje nutnost posouzení existenci vysokého rizika v pravděpodobných situacích, naopak pro nutnost posouzení zde zcela postačí riziko prosté.[137]

Podstatou DPIA je tedy posouzení rizik, která mohou, v určitých pravděpodobných situacích v souvislosti umístění osobních dat do datapoolu, nastat. Součástí takovéhoto posouzení je i plán jak takováto rizika omezit či úplně odstranit a jak postupovat v případě že k určité situaci i přes všechna opatření dojde. Mezi společensky chráněné zájmy na něž má být dopad posuzován pak podle WP 29 patří zejména práva na ochranu osobních údajů a soukromí, do skupiny ohrožených práv lze ale řadit i právo na svobodu projevu, svobodu myšlení, svobodu pohybu, zákaz diskriminace, právo na svobodu svědomí a náboženské vyznání.[138] [139]

3.4.1 Kdy je DPIA požadováno

V souladu s článkem 35 GDPR je DPIA vyžadováno v případech kdy "*je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob*."[140] Jedná se zejména o případy kdy dochází k rozsáhlému, systematickému u zpracování osobních údajů za účelem automatizovaného vyhodnocování včetně profilování a kdy jsou na takovýchto závěrech závislá rozhodnutí, která mají na fyzické osoby právní účinky a nebo vyvolávají následky s podobně závažným dopadem.[141]

---

[137] KOSTA, Eleni in Christopher, BYGRAVE, Lee, DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU General Data Protection Regulation (GDPR); A Commentary*. Oxford University Press, 2020. ISBN 978–0–19–882649–1. Strana 670.

[138] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strana 7

[139] Článek 8 Evropské úmluvy o ochraně lidských práv

[140] Odstavec 1 článek 35 GDPR

[141] Článek 35 odst. 3 písmeno a) GDPR

Dalším případem, kdy je zpracování DPIA nezbytné jsou případy ve kterých dochází ke zpracování údajů v čl. 9 odst. 1 GDPR a údajů o týkajících se trestných činů uvedených ve článku 10 GDPR.

Další upřesnění a rozšíření těchto základních bodů je pak v kompetenci jednotlivých dozorových úřadů[142] na vnitrostátní úrovni, kteří v souladu s čl. 35 odst. 4 "*sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů*."

Z důvodu předchozí zkušenosti, kdy jednotliví dozorových úřadů z důvodu přehlcení[143] Samotná WP29 pak uvedla ve svých guidelines seznam devíti bodů, indikujících vysoké riziko zpracování přičemž v situaci kdy zpracování splňuje alespoň dvě z oněch devíti je automaticky dovozováno, že se jedná o činnost spadající do činností dle čl. 35 odst. 1 a DPIA je zde vyžadováno automaticky.

V případě, že by ani s ohledem na výše uvedené nebylo zcela jasné, zda je v konkrétním případě posouzení vlivu na ochranu osobních údajů požadováno, uplatní se *pravidlo in dubio pro* DPIA.

3.4.1.1 Kritéria obligatorního DPIA dle WP29

Jak již bylo nastíněno WP29 ve svých pokynech k DPIA konkretizovala nařízením daný demonstrativní výčet situací, kdy je nutné zpracovat DPIA na devět bodů u nichž se předpokládá že kumulativní splnění alespoň dvou[144] z nich zakládá stejnou povinnost. Jedná se o použití technik hodnocení nebo bodování, automatizovaného rozhodování, které má právní nebo podobně závažný dopad, systematického monitorování, zpracování citlivých údajů a nebo údajů vysoce osobní povahy, zpracovávání údajů v rozsáhlém měřítku, přiřazování nebo slučování datových souborů, zpracovávání údajů týkajících se zranitelných subjektů osobních údajů, nové použití nebo využití nových technologických nebo organizačních řešení a případy kdy samotné zpracování "*brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či*

---

[142] Ve smyslu čl. 51 GDPR

[143] Toto přehlcení DPO je závažným problémem, který přetrvává dodnes.

[144] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. strana 12

smlouvy."[145] [146] Některá z těchto však kritérií bývají v kontextu datapoolingu splněna téměř pokaždé, zatímco jiná nabývají v případě splnění zcela nový rozměr. Níže proto budou jednotlivá kritéria podrobněji rozebrána.

Pravděpodobně nejzásadnějším kritériem v kontextu datapoolingu je *přiřazování nebo slučování datových souborů*. Vycházejme z toho, že s ohledem na princip vzájemnosti sdílení, jakožto jednoho z definičních znaků datapoolingu,[147] bude sdílení dat v datapoolu zásadně splňovat toto kritérium, neboť zde budou sdílena data minimálně od dvou zdrojů - stran smlouvy. Výjimkou z tohoto pravidla by mohla být snad pouze situace, kdy by takovéto spojování údajů nepřesahovalo přiměřené očekávání[148] subjektů údajů.[149] Takovéto přiměřené očekávání pak bude korespondovat s právním základem pro zpracování osobních údajů subjektu. V praxi tak bude záležet na tom na jakém právním základě jsou data zpracována a zda lze přiměřeně očekávat, že budou daným způsobem zpracovávána v datapoolu. Obecně lze však říci, že situace, ve kterých bude přiměřené od subjektu očekávat komplexní zpracování dat v rámci datapoolu, bude nastávat pouze u dat získaných za účelem vědeckého výzkumu.[150]

Dalším přímo navazujícím aspektem, který bude relevantní zejména pro větší datapooly, bude kritérium vztahující se na údaje zpracovávané v rozsáhlém měřítku. GDPR v tomto smyslu přesnou definici nezná, nicméně WP29 ve dovozuje z odstavce 91 odůvodnění GDPR čtyři výkladové faktory, jimiž jsou: "*počet dotčených subjektů údajů vyjádřený konkrétním číslem, nebo jako podíl příslušné populace; objem údajů a/nebo rozsah jednotlivých zpracovávaných*

---

[145] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strany 10 - 12

[146] Odstavec 91 odůvodnění GDPR

[147] Viz. výše v úvodu kapitoly Datapooling jako technika

[148] Odstavec 47 odůvodnění GDPR

[149] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strana 12 bod 6

[150] Tento poje není v GDPR definován v souladu s Pokyny pro souhlas podle nařízení 2016/679 str. 28 a 29 je však potřeba vykládat tento pojem spíše extenzivně nicméně stále v souladu s běžnými odvětvovými a etickými standardy.

údajů; délka nebo trvání činnosti zpracování údajů; zeměpisný rozsah činnosti zpracování."[151]

Rozsah zpracování nepřímo implikuje kritérium nového použití nebo využití nových technologických nebo organizačních řešení. Vzhledem k faktu, že naprostá většina nových technologií v IT spočívá v efektivnější organizaci dat a využívání výhod spočívajících v kreativitě jejich kombinací, je pak takovéto zpracování časté a žádoucí. Kvalitní a novátorská práce s daty bývá velmi čato jednou ze zásadních ingrediencí udržení si konkurenční výhody a jedním z důvodů proč spolu jednotlivé strany DSA datapool vytvářejí.

Dalším stupněm využití technologií v datapoolu a zároveň jedním z kritérií je automatizované rozhodování, tj. *rozhodování které má právní nebo podobně závažný dopad*[152]. Toto kritérium bude splněno pokaždé, když budou osobní údaje shromážděné v datapooolu používány alespoň jednou ze stran jako podklady k rozhodování, které má pro subjekt osobních údajů právní následky a nebo následky, které mají na subjekt podobně závažný dopad. Příkladem následků v takového rozhodnutí, které sice nevyvolává právní účinky, ale má na subjekt osobních údajů srovnatelný dopad je například poskytování úvěru bankou. Výše zmíněné se ovšem uplatní pouze pokud není takovéto zpracování plně automatizované[153] a do celého procesu alespoň jednou zasáhne smysluplným způsobem lidský faktor. Nestalo-li se tak, spadne takovéto plně automatizované zpracování (obvykle umělou inteligencí) pro účely kritérií DPIA do kategorie nového použití a *využití nových technologických nebo organizačních řešení,* o které jsme již hovořili výše.

Dalším kritériem, které se váže k sestavování profilu jedince je kritérium *hodnocení nebo bodování*, kdy na základě dat použitých v datapoolu bude docházet za účelem vyhodnocení dat k sestavování profilů v rámci nichž budou analyzovány nebo jinak vyhodnocovány osobní aspekty jako jsou pracovní výsledky, osobní preference, zájmy, spolehlivost, chování, zdravotní stav nebo

---

[151] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. strana 12

[152] Článek 35 odst. 3 písm. a) GDPR

[153] Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 přijaté dne 3. října 2017, ve znění naposledy revidovaném a přijatém dne 6. února 2018 Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Kapitola VI strana 30

místo pobytu či pohybu.[154] Klasickým příkladem datapoolu splňující toto kritérium tak budou například ATS[155] se sdílenou databází zájemců o pracovní místa v daném oboru a jejich případné hodnocení z předešlých zaměstnání. Dalším případem, kdy by datapool mohl toto kritérium splňovat je sdílený seznam zaměstnanců, kteří mohou poskytovat rady ohledně určitých okrajovějších specializací napříč společnostmi.

Datapooly ukládající data subjektů osobních údajů který jsou spíše osobnějšího rázu rovněž mohou splnit kritérium zpracovávání *citlivých údajů nebo údajů vysoce osobní povahy*. Tato kategorie osobních údajů je velmi pestrá, v zásadě se však bude jednat o údaje, které mohou ve srovnání se standardními osobními údaji *zvyšovat možné riziko pro práva a svobody jednotlivců*.[156] Do této kategorie osobních údajů tak budou mimo jiné vždy spadat osobní údaje podle článků 9 a 10 GDPR. Z hlediska datapoolingu jsou nejexponovanějšími osobnímu údaji z této skupiny zejména některá data shromážděná o uživatelích pomocí IoT (tákající se například vysoce osobních preferencí, chování jednotlivých členů domácnosti a v krajním případě některých chytrých asistentů také například politického smýšlení). Velmi specifickou skupinou dat, která spadají do kategorie údajů vysoce osobní povahy, které mohou být skladovány v datapoolech jsou rovněž tzv. *lifelogy*,[157] což jsou informace o denních aktivitách uživatele sbírané prostřednictvím nejrůznějších lifestylových aplikací jako je například Apple Health nebo chcete-li konkurenční HUAWEI Health či Samsung Health, Strava, HitMeal, Cronometer, MyFitnessPall a mnoho dalších.

Na monitorování aplikacemi pak navazuje kritérium *systematického monitorování* subjektů osobních údajů, v tomto případě však často nejde o monitorování jedno subjektu osobních údajů, ale celé skupiny. Kritérium systematičnosti pak sledování splňuje ve smyslu výkladu WP 29[158] takové sledování, které naplní alespoň jednu z následujících předpokladů; Monitorování

---

[154] Odůvodnění GDPR odstavec 71

[155] Z angličtiny Applicant Tracking System - systémy sloužící k vyhledávání a srovnávání vhodných žadatelů o zaměstnání.

[156] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strana 11

[157] Ibid.

[158] Viz. blíže Pokyny k funkci pověřence pro ochranu osobních údajů schválené dne 13. prosince 2016 Pracovní skupinou pro ochranu údajů zřízenou podle článku 29

se řídí určeným systémem, je předem naplánované, organizované nebo periodické, probíhá v rámci obecného plánu pro soubor údajů, je prováděno v rámci strategie. Společně s tím to alternativním výčtem pak musí monitorování probíhat ve veřejně přístupných prostorech.[159] Příkladně toto kritérium může v datapoolingu naplňovat zejména monitorování obchodních prostor, vyhodnocované pro účely marketingu. Toto kritérium je z hlediska zásahu doprav subjektu osobních údajů velmi významné zejména proto, že se mu začasté nelze efektivně vyhnout.[160] [161]

Co se týče zranitelnosti samotné, potřebu ochrany v tomto smyslu zdůrazňuje kritérium *údajů týkajících se zranitelných subjektů údajů*. V tomto smyslu je pak potřeba si uvědomit zda mezi kategorie dat skladovaných v datapoolu neshromažďují zejména údaje o zaměstnancích, osobách se sociálním znevýhodněním a nezletilých.

Posledním, kritériem je situace kdy zpracování „*brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy*"[162], tato kategorie se však vzhledem dle svého charakteru v podstatě odpovídá kategorii *rozhodování které má právní nebo podobně závažný dopad,* a odlišuje se od ní pouze nižší měrou závažnosti dopadu na reálný život subjektu osobních údajů.

3.4.2 Jak se DPIA provádí

V souladu s článkem 35 odstavcem 7 posouzení musí DPIA obsahovat alespoň systematický popis zamýšlených operací zpracování společně s případným odůvodněním oprávněných zájmů správců ke zpracování, posouzení nezbytnosti a přiměřenosti operací zpracování z pohledu účelu, kterého má být dosaženo, posouzení rizika které takovéto zpracování představuje pro práva a svobody subjektů osobních údajů jejichž data jsou zpracovávána a popis plánovaných opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření

---

[159] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strana 11

[160] Samozřejmě za předpokladu, že chceme žít životním stylem, který je v tzv. vyspělých zemích obvyklý.

[161] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strana 11

[162] Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Strana 12

a mechanismů k zajištění ochrany osobních údajů společně se zajištěním doložení souladu s GDPR.

Samotné provádění DPIA je přitom obvykle v praxi děleno do sedmi[163] dílčích kroků a sice identifikace potřeby DPIA provádět (jejíž aspekty byly popsány výše), popisu zpracování, zvážení konzultace externích entit, jako jsou poradenské společnosti anebo autority za tímto účelem zřizované členským státem, posouzení nutnosti a proporcionality zpracování, posouzení rizik takovéhoto zpracování, zpracování určité formy faktického výstupu, například v podobě posouzení plánu pro řízení rizik a závěrem celkové vyhodnocení výsledků DPIA, společně s konstatováním ohledně závažnosti odstraněných a přetrvávajících rizik a s informací o tom zda je na základě výsledků nutno dále kontaktovat příslušný orgán ochrany osobních údajů v daném členském státě.

Závěrem pouze zmiňme, že pokud jsou rámci výše nastíněného DPIA zjištěna rizika, které nelze odstranit a nebo alespoň s úspěchem minimalizovat, musí se správci provádějící DPIA obrátit na DPO a zpracování s ním konzultovat. DPO pak buď navrhne další možná opatření jak tato rizika dostatečně omezit, schválí takovéto zpracování i s přetrvávajícími riziky a nebo zpracování zcela a nebo z části zakáže.

3.4.2.1 Společné DPIA

V případě, že společní správci osobních údajů provádí rovněž společné DPIA, je nutné, aby si předem sjednali metodiku, podle které bude postupováno. Je potřeba mít na paměti, že při posouzení DPIA je nutné posoudit i rizika, která by mohla vzejít z interní firemní kultury jednotlivých společností a výsledný dokument tak může odhalit i vnitřní procesy společností jejichž odtajnění dalším společnostem v datapoolu může představovat ztrátu jistých konkurenčních výhod.

Za vhodnější alternativu tak lze považovat zpracování dílčích DPIA v jednotlivých společnostech, jejichž výsledek bude z části zveřejněn, tak aby nevznikaly pochybnosti o bezpečnosti zpracování dat a zároveň byla chráněna důvěrnost vnitřních procesů společnosti. Tato interní DPIA mohou být v jednotlivých společnostech prováděna na základě zákonné povinnosti, a nebo dobrovolně pouze za účelem možnosti demonstrovat partnerům v datapoolu

---

[163] The DPIA Process - a step-by-step guide. Online. Dostupné z: https://www.lboro.ac.uk/data-privacy/resources/dpia/dpia-process. [cit. 2024-03-31]. A dále How do we do a DPIA? Online. Dostupné z: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how12. [cit. 2024-03-31].

důvěryhodnost společnosti sdílející data. Na tato jednotlivá DPIA pak bude navazovat DPIA pokrývající rozsah společného zpracování v cloudu.

Pokud by se však správci přesto rozhodli zpracovat DPIA pro data zpracovávaná v cloudu společně bez navazujících dílčích posouzení, je potřeba velmi detailně předem ujednat meze zpracování DPIA v návaznosti na jednotlivé členy datapoolu tak, aby bylo DPIA způsobilé pokrýt odpovídajícím způsobem všechna rizika zpracování uvnitř dataopoolu a zároveň přenosy dat směrem dovnitř i ven z datapoolu a stanovit ochranu procesů probíhajících mezi získáním dat a jejich nahráním do datapoolu.

Součástí dohody o provádění DPIA musí rovněž být mechanismy a lhůty odstraňování rizik, která DPIA odhalí. U datapoolů tvořených většímu počtuem společností je rovněž vhodné ujednat podmínky za jakých mohou být v závislosti na neuspokojivém výsledku DPIA, na který nenaváže efektivní řešení v jednotlivých společnostech tyto společnosti z datapoolu dočasně a nebo úplně z datapoolu vyloučeny. Pro případ, že se bude neuspokojivý výsledek DPIA týkat přímo procesů zpracování uvnitř datapoolu je vhodné ujednat si rovněž kompetence, financování a lhůty pro případné řešení tak, aby byly jednotlivé strany datapoolu schopné splnit povinnosti, týkající se zpracování tak a dostát tak povinnostem společných správců.

4 Ochrana neosobních dat

Jak již bylo v této práci několikrát zdůrazněno, se stoupajícím významem dat pro společnost a jejich ekonomickým významem narůstá i jejich důležitost v obchodním styku. Z výše zmíněného pak plyne potřeba mnohem rozsáhlejších a propracovanějších konceptů ochrany. Tato ochrana pak musí být interní součástí všech mechanismů fungování datapoolu. Již dávno totiž neplatí, že kvalitní ochranu lze zajistit použitím odpovídajícího programového vybavení. Ba právě naopak, v dnešní době převážná část hackerských útoků necílí na zranitelnosti určitého softwaru, ale především na chybu lidského faktoru. Je to jednoduše proto, že lidský uživatel až do nedávna, narozdíl od softwarového vybavení, neprocházel testováním. Stále více společností chápe důležitost náležitého proškolení svých zaměstnanců, v rámci kterého jsou několikrát ročně informováni o nejnovějších kybernetických hrozbách, naučí se praktické tipy a triky na to jaká preventivní opatření učinit, jak rozpoznat nebezpečí a jak postupovat v krizových situacích,

tak aby bylo zamezeno co neefektivně dalším škodám a incident byl oznámen co nejrychleji k tomu najatým externím a nebo interním specialistům.

Při zvládání kybernetických incidentů jde přitom často hlavně o čas, který je zásadní při izolaci napadené části systémů od zbylých, nenakažených. Rychlý zásah minimalizuje ztráty a umožňuje rychlé obnovení plné funkčnosti služeb. Kybernetický incident tak lze přirovnat, s trochou nadsázky, k r šířícímu se požáru. I v tomto případě je rychlost reakce základním parametrem určujícím celkový objem škod. Byť při kybernetickém incidentu nehrozí ztráty na životech, materiální škody mohou mít mnohem vyšší dopad, požár totiž pravděpodobně nezpůsobí ztrátu důvěry zákazníků a obchodních partnerů, zatímco nevhodné zvládání kyberincidentu ano. Stejně jako v případě požáru je tak nutné i pro případ kyberincidentu natrénovat postupy, aby každý ze zaměstnanců společnosti, ale do jisté míry i zákazníků a obchodních partnerů, věděl, jak se chovat a co přesně dělat.[164]

V prostředí datapoolu je pak nutné aplikovat kyberbezpečnost ve svojí nejsofistikovanější verzi. Musí spolu totiž spolupracovat jak entity zajišťující údržbu hardware a software, který datapool používá, ale i jednotlivé společnosti podílející se na datapoolu, stejně tak jako všichni zaměstnanci, kteří s datapoolem interagují a v návaznosti na architekturu propojení s interními systémy společností podílejících se na datapoolů i všichni zaměstnanci těchto společností.[165] Ochrana proti kybernetickým hrozbám je totiž pouze tak kvalitní jak kvalitní je její nejslabší článek.

4.1 Ochrana neosobních dat v režimu NIS2

V souvislosti s výhodami, které poskytuje sdílení rozsáhlých souborů dat v datapoolech, mohou být tato datapooly velkým lákadlem pro nejrůznější útočníky. V případě získání dat jsou tato data cenou komoditou, kterou lze snadno prodat konkurenci. V případě jejich zaheslování pomocí ransomwaru je pak naopak velmi pravděpodobné, že budou společnosti ochotné platit nemalé částky aby k takovýmto datům získaly co nejdříve znovu přístup. Velké ekonomické ztráty pak může znamenat i odepření přístupu následkem DDoS útoku o úplném a trvalém vymazání ani nemluvě. K tomu všemu je pak nutné připočíst třeskutou

[164] Z dosavadní praxe autorky vyplývá, že se stále nemalá část uživatelů domnívá že stačí vytrhnout napadené zařízení ze zásuvky. Popřípadě je vypnout. Takovéto řešení však může být velmi často fatální.

[165] I ti co s datapoolem nepracují.

geopolitickou situaci a zjistíme, že pro to aby byl datapool bezpečnou a vítanou součástí ekonomiky, musí být především velmi kvalitně a zodpovědně zpracován po stránce technické.

Tato nutnost pak nezůstává v rovině pouhých technických požadavků, ale rovněž se přesouvá do roviny právní a to společně s vydáním směrnice (EU) 2022/2555 ze dne 14. prosince 2022 tzv. NIS 2, která meritorně nahradila NIS dokument (EU) 2016/1148.[166] Už samotný fakt, že tak velké a legislativně komplikované těleso jako je Evropská Unie přikládá nějakému tématu takovou důležitost a vážnost, že najde politickou schodu k aktualizaci směrnice během pouhých pěti let, pak o tomto tématu pak vypovídá mnohé. I přesto, implementace této směrnice do jednotlivých právních systémů v současné době teprve začíná probíhat a její kompletní finalizace fungování je ve spolupráci s Komisí plánována až na 17 října 2027,[167] již dnes může být důležitým zdrojem pro položení základů kvalitního a udržitelného konceptu kyberbezpečnosti v datapoolingu.

Prvním a pro budoucí fungování datapoolů pravděpodobně nejzásadnějším aspektem, který NIS 2 přináší je vymezení dvou skupin na které se budou povinnosti vztahovat, na tzv. základní[168] a důležité[169] subjekty. Přičemž datapooly, na kterých se podílí střední a velké podniky budou dopadat pravidla týkající se důležitých subjektů. Otázkou, která je v tomto okamžiku ponechána nadcházející praxi a národním úpravám jednotlivých členských států, zůstává, zda nebude v tomto případě datapool, byť postrádající právní subjektivitu, posuzován jako jedna souborná entita ve smyslu NIS2. V takovémto případě by například bylo možné limity pro posouzení zda se jedná o datapool velký a střední hodnotit, pro zaměstnance a obraty všech společností dohromady, čímž by se rozsah datapoolů spadajících do regulace NIS2 významně zvýšil. Nad rámec výše zmíněného je pak ponecháno v kompetenci jednotlivých členských států jaký

---

[166] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

[167] Článek 40 Ibid.

[168] V anglickém originále *essential*

[169] V anglickém originále *important*

okruh entit zahrnou do kategorie důležitých subjektů, ovšem vždy s ohledem na minimální okruh stanovený NIS2.[170]

Stejně jako GDPR i NIS2 zakotvuje svůj vlastní systém obligatorního posouzení kybernetických rizik zakotvený v článku 21, který zakotvuje povinnost subjektů podléhajících NIS2, přijmout odpovídající opatření v závislosti na aktuálně dostupných technologiích a informacích ohledně kyberbezpečnosti. "*Při posuzování přiměřenosti těchto opatření se náležitě zohlední míra vystavení subjektu rizikům, velikost subjektu a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a hospodářského dopadu*."[171]

Samotné posouzení pak v souladu s odstavcem 2 článku 21 NIS2 musí zahrnovat pravidla bezpečnosti informačních systémů a analýzy rizik, způsoby zvládání incidentů, pravidla pro krizové řízení včetně kontinuity provozu, řízení zálohování a zotavování po kybernetickém incidentu, bezpečnost dodavatelského řetězce, bezpečnost při pořizování, pravidla vývoje a údržby sítí informačních systémů, včetně řešení a zveřejňování zranitelností, zásady a postupy při hodnocení účinnosti opatření pro řízení rizik v oblasti kybernetické bezpečnosti, základní postupy v oblasti kybernetické hygieny a školení v oblasti kybernetické bezpečnosti, zásady a postupy týkající se používání kryptografie a šifrování, bezpečnost lidských zdrojů, zásady přístupu a správy aktiv a používání vícfeaktorové autentizace a řešení průběžného ověřování, zabezpečené hlasové, video a textové komunikace a případně i zabezpečení systémů nouzové komunikace v rámci subjektu.

Trojici nejdůležitějších novinek, které budou muset datapooly v rámci NIS2 splňovat pak uzavírá povinnost včasného hlášení kybernetických incidentů k tomu určeným orgánům členských států tak, aby byla možná vnitrostátní ale i mezinárodní koordinace rizik.

Závěrem je k NIS 2 vhodné zmínit, že v případě, kdy se bude jednat o datapool skladující data ve více členských státech Evropské unie, bude muset tento datapool v rozsahu skladovaných dat na základě principu datové suverenity splňovat pravidla, která stanoví členský stát, na jehož území se daná část

---

[170] Odůvodnění odst. 17 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

[171] Článek 21 odst. 1 NIS 2 Ibid.

datapoolu nachází a zároveň pravidla států, ve kterých mají jednotlivé společnosti tvořící datapool sídlo.[172]

5. Ochrana hospodářské soutěže

Vytváření rozsáhlých datapoolů je obvykle vnímáno pozitivně z hlediska rozšíření možností jeho účastníků a tím umožnění efektivnějšího fungování společností a jejich celkové prosperity. Ve stejném duchu se rovněž vyjadřuje Evropská Komise, která ve své Digitální strategii EU pro období mezi lety 2019 a 2024 jasně hovoří o tom, že "*Přístup k datům a schopnost je využívat jsou zásadní pro inovace a růst*."[173] [174]

Odvrácenou tváří datapoolů je však jejich schopnost narušit fungování hospodářské soutěže. V praxi může dojít k tomu, že kvalitní datapool přístupný pouze pro jeho účastníky, bude představovat na trhu výhodu, která bude pro ostatní subjekty na trhu likvidační, protože společnosti v souvislosti s využíváním datapoolu disponují "*obrovským množstvím dat a zároveň mají technickou kapacitu a kvalifikovaný personál pro jejich analýzu, získají konkurenční výhodu*.[175] [176]

V současné době i přes politickou "podporu" vytváření datapoolů, není stanoven konkrétní rámec toho, kdy jsou datapooly legální a vítané a kdy se jedná o nežádoucí praxi, která může mít za následek vyloučení či omezení hospodářské soutěže.[177] Při vytváření sdílených datapoolů tak společnosti často nedobrovolně

---

[172] Popřípadě pravidla členského státu, ve kterém má datapool s vlastní právní subjektivitou sídlo.

[173] EVROPSKÁ KOMISE. *European data strategy: Making the EU a role model for a society empowered by data. Online*.

[174] LEXOLOGY. *When is data pooling anticompetitive?*

[175] OECD. *Data-Driven Innovation: Big Data for Growth and Well-Being.*

[176] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů s názvem Směrem ke společnému datovému prostoru ze dne 25. dubna 2018

[177] Evropská Komise je v souvislosti se zmíněnou problematikou toho názoru, "*…že v této fázi vývoje ekonomiky založené na datech odpovídá stávající předpisový rámec svému účelu a že je zatím příliš brzy na horizontální právní předpisy o sdílení dat ve vztazích mezi podniky…*" Autorka se však nedomnívá, že by platný právní rámec EU zajišťoval dostatečnou právní jistotu již v roce 2018, kdy byl tento názor prezentován, tím méně dnes v roce 2024, téměř šest let od vydání, kdy se právní stav bohužel zásadně nezměnil. (Viz.Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů s názvem Směrem ke společnému datovému prostoru ze dne 25. dubna 2018.) Jediným jakýmsi částečným posunem je DMA, které v určitém rozsahu stanovuje podrobnější pravidla pro datové společnosti, která se na datapool aplikují pouze v případě, že má samostatnou právní subjektivitu.

riskují nejen pokuty ale i povinnost data nacházející se v datapoolech zveřejnit. Takováto povinnost data zveřejnit pak může mít pro společnosti na dnešním informacemi poháněném trhu fatální účinky. Výše zmíněné riziko pak může společnosti i přes značné ekonomické benefity datapoolingu od zakládání datapoolů efektivně odradit. V následující kapitole této práce se tak pokusíme, alespoň z části onu hranici nalézt a nebo alespoň vymezit určitá kritéria rozlišení.

5.1 Vymezení podmínek pro vznik škodlivého efektu na hospodářskou soutěž

Základním předpokladem pro určení, zda se jedná o datapool se škodlivým efektem je určit, zda jsou strany anebo alespoň některé z nich sobě navzájem potenciálními soutěžiteli. *Společnost se považuje za potenciálního soutěžitele jiné společnosti, je-li při neexistenci dohody v případě malého, avšak trvalého zvyšování relativních cen pravděpodobné, že tato prvně uvedená společnost v krátké době uskuteční potřebné dodatečné investice nebo vynaloží jiné nezbytné náklady přechodu za účelem vstupu na relevantní trh, na němž působí jiná společnost*.[178]

Tato definice je problematická hned z několika důvodů. Pravděpodobně nejzásadnějším z nich je složitost vymezení relevantního trhu, které je v případě datapoolů extrémně složité. Jednotlivé společnosti samy o sobě formálně nemusí být z hlediska obvyklého posouzení soutěžiteli a přesto může mít datapool povahu kartelové dohody například v tom smyslu, že se společnosti na různých relevantních trzích spojí a způsobí tím škodu (ať už záměrně a nebo mimoděk) na třetím relevantním trhu, který však s původními trhy dle konvenčního vnímání vůbec nesouvisí. Relevantní trh jako takový je přitom velmi složité vzhledem k rozsahu a množství možností použití dat schraňovaných v datapoolu prakticky nemožné určit. Jistě existují trhy, které budou vzhledem k oborům podnikatelské činnosti společností tvořících datapool bezesporu trhy relevantními, a naopak trhy, které bezesporu relevantními pro datapool nejsou, nicméně zde vzniká ve srovnání s tradičně posuzovanými odvětvími až neproporčně široká šedá zóna.

Samotné jádro problémů vyplývajících z této definice v datapoolingu pak spočívá v tom, že se jedná o definici, která je orientovaná na výsledek (Pokud společnost udělá krok A, pak se společnost vynaloží investice či náklady), zatímco

[178] Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci 14. ledna 2011 Komisí. Bod 10

samotný datapooling je založený spíše na ukotvením procesů spočívajících v získávání a zpracovávání dat. U tohoto procesu se pak konkrétní výstupy v závislosti na cílech společností a dostupných technologiích a strategiích zpracování, dynamicky vyvíjí. Připočtěme k tomu rovněž okruh společností tvořících DSA, který se také zpravidla velmi rychle mění a to často i v řádech hodin či dnů. Proto bohužel není nadsázkou tvrdit, že určit v případě datapoolů relevantní trh je úkolem spíše než pro právníka či ekonoma úkol hodný spíše pouťového věštce. Tento efekt pak zplna neodstraní ani pravidelné vyhodnocování trhu, které se bude často dít až následně. Rovněž frekvence takovéhoto vyhodnocování nemůže být dostatečná a zároveň ekonomicky udržitelná. Zejména velké a strukturálně sofistikované datapooly tak v praxi dennodenně balancují nedobrovolně na hraně zákona.

Nicméně, vraťme se k původní definici soutěžitelů a zmiňme, že tato se nebude rovněž vztahovat na vnitropodnikové datapooly a datapooly ve vzájemně závislých společnostech na které se uplatní výjimka ve smyslu odstavce 3 článku 101 SFEU. Na základě této podmínky je možné prohlásit odstavec jedna za neúčinný pro určité kategorie toho mezi podniky a rozhodnutí nebo kategorie rozhodnutí činěná sdružením podniků. Zde bude následně posuzována zejména úroveň spojení jednotlivých podniků.[179]

Pokud již dojdeme k závěru, že jsou si společnosti, které společně vytváří datapool soutěžiteli, je nutné se zaměřit na to jaký efekt o jaké intenzitě má daný datapool na trh. Demonstrativní výčet fakultativně splnitelných škodlivých prvků je přitom ve svojí obecné verzi poskytován odstavcem prvním, článku 101 SFEU. Při vyhodnocování, zda má datapool škodlivý vliv na hospodářskou soutěž, je rovněž nutné do posouzení zahrnout, zda neexistují pozitivní účinky, které by jisté negativní účinky vyvažovaly.[180] Jak ostatně stanovil SDEU v rozsudku AC Treuhand: Je v konkrétním případě *"totiž nejprve třeba vzít v úvahu celkový kontext, ve kterém byla uvedená dohoda nebo uvedené rozhodnutí přijaty nebo ve kterém mají své účinky, a konkrétněji jejich cíle…*"[181] Tento zdánlivě jasný úkol dále komplikuje fakt, že v neexistuje žádné vodítko, které by určovalo, míru

---

[179] Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 18. září 2001 ve věci M6 and Others v Commission. Bod 74.

[180] Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 6. října 2006 ve věci GlaxoSmithKline Services and Others v Commission and Others. Bod 95.

[181] Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 8 července 2008 ve věci AC-Treuhand v Commission. Bod 126.

pozitivity či negativity daného efektu na hospodářskou soutěž. Samotný výsledek je v následku toho nutně arbitrární, závislý na pohledu, postavení a zkušenostech lidského faktoru a to zejména s přihlédnutím k tomu, že datapooly jako fenomén umožňují některé přelomové funkce moderních technologií a názory na tyto technologie samotné se napříč společností velmi liší. Konkrétní názor regulátora při kontrole tak lze opět spíše hádat nežli předpovídat. I přesto a nebo právě proto se níže pokusíme zaměřit na klíčové aspekty a stanovit alespoň jakési dílčí milníky a to jak z hlediska postavení soutežitelů, tak efektu, které jednotlivé případy přináší.

5.1.1 Horizontální a vertikální působení

Co se týká hospodářské soutěže, lze rozdělit možný negativní vliv dohod obsažených jak v DSA, tak v separátních dokumentech[182], na horizontálních tak vertikálních DSA, kdy se jednotlivé druhy ujednaní budou lišit podle toho jakou roli hrají dodavatelském řetězci. Vzhledem ke komplexitě některých ujednání může rovněž docházet k vytváření datapoolů, které budou mít jak horizontální tak vertikální působení zároveň.

5.1.1.1 Vertikální působení datapoolů

V případě vertikálního sdílení dochází pomocí DSAa přidružených dokumentů k propojení dvou a více vrstev trhu. Například vznikne datapool, který výrobci umožní získávat od distributorů poznatky týkající se preferencí koncových zákazníků a od dodavatelů informace o dostupnosti, ceně a možnostech technických řešení a surovin. Tento typ datapoolingu se zdá všestranně výhodný, neboť zákazníci dostávají produkty, které lépe odpovídají jejich potřebám, distributorům se pak v důsledku tohoto zvýší zisky z prodeje, zatímco výrobci a dodavatelům stoupá odbyt. Výrazně se rovněž zlepší flexibilita trhu v případě výpadků dodávek určitých produktů a nebo služeb. Odvrácenou stranou mince je však fakt, že kdokoli bude stát mimo tento datapool může mít významně ztíženou pozici na trhu. Klasickým příkladem takovéhoto převážně vertikálního ujednání týkajícího se předchůdce datapoolů jak je známe dnes, je rozhodnutí ve věci John Deere Ltd proti Komisi[183] ve kterém … I přesto je však

---

[182] Tyto separátní dohody pak vůbec nemusí být uzavírány s vědomím všech stran podílejících se na datapoolu.

[183] Rozsudek pátého senátu Soudního dvora Evropské unie ze dne 28. května 1998 ve věci John Deere Ltd. v Commission

vnímáno riziko narušení hospodářské soutěže pomocí vertikálně působícího ujednání ve srovnání s horizontálním, jako poměně nižší.[184]

Bližším vodítkem pro stanovení rozlišení míry škodlivosti/či prospěšnosti je bloková výjimka v nařízení VABER,[185] které specifikuje podmínky odst. 3 článku 101 SFEU pro účely vertikálních dohod. Hlavním úhelným kamenem této blokové výjimky je stanovení stanovení konkrétní monetární hranice, pod kterou nemůže mít datapoolu s vertikálním efektem dostatečně významný negativní efekt na hospodářskou soutěž. Článek 2 odstavec 2 VABER stanoví tuto hranici pod kterou dohoda s vertikálním omezením automaticky spadá dohoda do rámce odst. 3 článku 101 SFEU na 50 milionů EUR. Co se týče proporčního zastoupení dodavatelů na trhu, stanoví tuto hranici článek 3 odstavec 1 VABER na 30%.

Nicméně jak správně podotýká Kellerbauer[186] mohou nastat i situace, které nespadají do výjimek vyjmenovaných ve VABER a přesto spadají do rámce výjimek který lze podřadit pod článek 101 odst. 3 SFEU, protože škodlivá ujednání lze definovat podle cíle je nutné vykládat restriktivně a v případě nejasností musí být vždy posuzovány konkrétní účinky na trh.[187]

Prospěšný datapool může vznikat i v případech kdy velký výrobce určité technologie sdílí informace ohledně rozdělení potenciálních zákazníků a na základě tohoto dochází k rozdělení oblastí ve kterých budou působit jednotliví autorizovaní distributoři. Nicméně v tomto případě je nutné aby povaha daného výrobku a nutnost jeho vysoce kvalifikovaného servisu odůvodňovala takovýto cloud.[188] Obecně je rovněž vhodné aby byly stanoveny co nejvstřícnější podmínky pro vstup do takovéhoto datapoolu a zveřejní informací o jeho existenci pro případ zájmu nového subjektu, který je schopen splnit dané technické kvality. Beze vších pochybností tak lze konstatovat, že bez použití datapoolu je u jistých

---

[184] KELLERBAUER, Manuel; KLAMERT, Marcus a TOMKIN, Johnathan (ed.). T*he EU Treaties and the Charter of Fundamental Rights. A Commentary*. Oxford university press, 2019. ISBN 978–0–19–879456–1. Strana 1193, bod 63.

[185] Nařízení Komise 2022/720 ze dne 10. května 2022 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie vertikálních dohod a jednání ve vzájemné shodě

[186] KELLERBAUER, Manuel; KLAMERT, Marcus a TOMKIN, Johnathan (ed.). T*he EU Treaties and the Charter of Fundamental Rights. A Commentary*. Oxford university press, 2019. ISBN 978–0–19–879456–1. Strana 1016.

[187] Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 11 září 2014 ve věci CB v Commission. Bod 58.

[188] KELLERBAUER, Manuel; KLAMERT, Marcus a TOMKIN, Johnathan (ed.). T*he EU Treaties and the Charter of Fundamental Rights. A Commentary*. Oxford university press, 2019. ISBN 978–0–19–879456–1. Strana 1017, bod 69.

specifických případů globálních výrobců takovéto jednání prakticky nemožné.[189] Co se týče účinku takovéhoto datapoolu, musí být prokazatelný pozitivní efekt na zvýšení úrovně služeb či dostupnosti zboží daného výrobce u kterého by nebylo možné a nebo pravděpodobné bez vynaložení disproporčně vysokých finančních nákladů.

5.1.1.2 Horizontální působení datapoolů

V případě horizontálního DSA bude docházet ke sdílení dat mezi společnostmi, které se nacházejí na stejné úrovni trhu. Tyto dohody mají velký potenciál co do podpory rozvoje technologií a zkvalitnění služeb v určitém sektoru či odvětví. Za pomocí datapoolů je možné snížit plošně rizika a ušetřit náklady, které by jinak byly proinvestovány zbytečně a nebo se sdílet část know-how.[190] Negativním aspektem může být již zmíněné narušení cen a odstříhnutí některých hráčů na trhu od praktické možnosti účasti na hospodářské soutěži. To vše se může dít prostřednictvím zejména přímého a nebo nepřímého určování kupních cen na základě vzájemné koordinace skrze datapool, omezení nebo kontroly výroby, odbytu, dovozu, vývozu, omezení výzkumu a vývoje a nebo nuceného alokování investic, či rozdělení trhu nebo nákupních zdrojů.[191] Níže proto budou rozebrány vybrané oblasti horizontálních dohod z pohledu datapoolingu spolu se stručným rozebráním specifik, která z pohledu datapoolingu přináší.

5.1.1.3 Sdílení práv k převodu technologií

Prvním z pohledu vztahu datapoolingu a hospodářské soutěže pravděpodobně nejzajímavějším, je datapool technologický, ve kterém podniky sdílejí licence či know how týkající se technologií. V takovémto případě by byly za normálních okolností v případě uzavírání jednotlivých dvoustranných dohod chráněny dotyčné blokovou výjimkou TTBER.[192] [193] Ve sdělení k tomuto nařízení

---

[189] Rozsudek Soudního dvora Evropské unie ze dne 25. října 1977 ve věci Metro v Commission

[190] Více například viz. Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci 14. ledna 2011 Komisí.

[191] RABAN, Přemysl, a kol. *Obchodní právo.* Brno. Václav Klemm - Vydavatelství a nakladatelství, 2020. ISBN 978-80-87713-19-8. Strana 108.

[192] Nařízení Komise (EU) č. 316/2014 ze dne 21. března 2014 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie dohod o převodu technologií

[193] Tato bloková výjimka se uplatní na podniky uzavírající jednotlivé dvoustranné dohody o převodu technologií a zároveň podniky uzavírající dvoustrannou dohodu nedosahují společného podílu na relevantním trhu 20% a nebo 30% v případě podniků jež nejsou soutěžícími podniky.

je však přímo uvedeno, že se tato výjimka na většinu datapoolů z důvodu vícestranného charakteru DSA pro datapooly nevztahuje. Komise však v tomto dokumentu rovněž nastiňuje svůj postoj ke vzniku takovýchto datapoolů a poskytuje sérii vodítek jak postupovat v případě technologických datapoolů tak aby nepoškozovaly hospodářskou soutěž a tudíž spadaly do rámce článku 101 odst. 3 SFEU.

Pro úplné pochopení postoje Komise prezentovaného ve sdělení, je nutné na úvod zdůraznit, že se jedná o dokument vydaný v roce 2014 od kterého v době vzniku této práce uplynulo již téměř 10 let. Pokrok zaznamenaný ve světě informačních a komunikačních technologií je za tuto dobu nesmírný. Navíc vývoj některých z nich nabral zcela jiný směr než bylo předpokládáno. Svou hodnotu co se týče názorů a postojů komise však dokument jistě má a to zejména s ohledem na to, že jakýkoli oficiální zdroj novějších informací pro výkladovou praxi ze strany Unie absentuje. S ohledem na velmi imperativní lingvistickou strukturu části týkající se "technologických poolů," která svým řazením a definováním jednotlivých pojmů v podstatě kopíruje obsahovou strukturu závazných blokových výjimek, lze zde prezentovaný názor přinejmenším použít jako jakési vodítko.

Je rovněž vhodné zmínit, že sdělení vnímá datapooling pouze úzkou optikou technologických datapoolů, které jejich uživatelům umožňují na jednom místě a za jednu cenu, přístup k technologickým licencím. Část subjektů v datapoolu je tak čistými poskytovateli licence k softwaru a další část jsou recipienti, kteří těží z přístupu k souboru licencovaného obsahu, který je jim nabízen z pravidla výhodněji než by tomu bylo v situaci, kdy by nakupovali jednotlivé licence samostatně. Níže si pro rozebereme maxima obsažená ve sdělení Komise k TTBER a doplněná o možné analogické aplikace pro ostatní kategorie poolů.

K vytvoření technologického datapoolu, který bude v souladu s pravidly pro hospodářskou soutěž, je podle Komise potřeba plnit několik kritérií. Tato kritéria, zejména pokud jsou splněna kumulativně jsou z pohledu Komise spolehlivými ukazateli prokazujícímu pozitivní efekt datapoolu na trh. Prvním z nich je samotná povaha licencí a sice to, zda jsou si jednotlivé licence komplementy a nebo substituty a vztah licencovaných technologií s technologiemi mimo datapool. Proto sdělení zavádí dvojí rozlišení technologií sice na

technologické komplementy a technologické substituty, a dále na technologie postradatelné a nepostradatelné.[194]

Technologie jsou si komplementy pokud jsou zároveň potřebné k výrobě daného výrobku a to i v případě že se částečně jejich použití překrývá. Pokud by ale bylo možné si při výrobě daného produktu mezi technologiemi vybrat, bude se jednat o substituty. Důležitost tohoto dělení pak z pohledu komise spočívá v tom, že účelem technologického poolu, je hromadný nákup licencí a jejich následné postoupení v podobě získání přístupu ke cloudu. Pokud by byly do cloudu nakupovány licence, které by se navzájem mohly nahrazovat, znamenalo by to, že se ztrácí pozitivní efekt pro uživatele, kterým je získání levného přístupu k technologiím a převažuje negativní efekt v podobě omezení hospodářské soutěže. Jednalo by se totiž technicky vzato o kolektivní prodej. Určitou pozitivní indikací faktu, že se skutečně jedná o prospěšný datapool je také fakt, že poskytovatelé licence mohou danou licenci prodávat i mimo datapool a společnosti tak mají možnost volby, zda zvolí zakoupení jednotlivých licencí anebo raději zaplatí poplatek za užívání datapoolu. Fakultativně pak může být datapool ochoten prodávat licence na technologie zvlášť a to za předpokladu, že součet poplatku za jednotlivé licence nepřekročí poplatek za užívání celého datapoolu.

Druhým kritériem je vztah s technologiemi mimo datapool. Prospěšný datapool se vyznačuje tím, že technologie v něm seskupené jsou nepostradatelné pro výrobu předmětného výrobku a nebo pro takovou výrobu výrobku při které si výrobek udrží určitý standard, který je datapoolem podporován. Slovo *nezbytnou* v tomto kontextu znamená, že za technologii neexistuje žádný vhodný substitut.[195]

Dalším ukazatelem může být to, do jaké míry se podílejí na výběru technologií do datapoolu nezávislí odborníci. Dle komise se tak posiluje právní jistota ve smyslu záruky, že tyto osoby vyberou skutečně nejvhodnější řešení pro zákazníky datapoolu, bez ohledu na ekonomický zájem jiných subjektů. V tomto bodě nelze než názor Komise odmítnout. Vzhledem ke skutečné situaci na trhu, kdy nejpovolanější osoby v oboru bývají zaměstnávány na finančně zajímavých místech, která si ale mohou dovolit nabízet zejména velké korporace, nebo samy

---

[194] Sdělení Komise Pokyny o použití článku 101 Smlouvy o fungování Evropské unie na dohody o převodu Technologií. Bod 250.

[195] Sdělení komise k TTBER dokonce uvádí termín schůdný, cože je dle názoru autorky práce poněkud nešťastné. Schůdné řešení totiž mnohdy neznamená řešení dobré. Viz. Sdělení Komise Pokyny o použití článku 101 Smlouvy o fungování Evropské unie na dohody o převodu Technologií.

velké datapooly, by mělo být posuzováno spíše spektrum zapojených entit nežli jejich formální nezávislost. Jistým východiskem pro kontrolu kvality cloudu by pak de lege ferenda mohla být dokumentace, která volbu jednotlivých řešení osvětlí. Z funkčního hlediska pak rovněž často bývá cennější praktická znalost než formální odbornost.

Jedním z rizik technologických datapoolů, vzhledem k množství chráněných patentů, je fakt, že mohou obsahovat i patenty, které jsou již neplatné. Vytvoření datapoolu, obsahujícího byť jen jeden neplatný patent pak může mít za následek zvýšení nákladů na provozování datapoolu placením vyšších licenčních poplatků. V takovém případě, může datapool bránit inovaci v oblasti, které se týká a v důsledku toho se vystavovat riziku napadení v souladu s článkem 101 odst. 1 SFEU.[196] Nicméně v tomto bodu výkladu si v rámci svého sdělení sama Komise není jistá a bude proto záviset na konkrétní soudní praxi. De lege ferenda se však autorka domnívá, že by bylo výkladově vhodné spíše posuzovat převážný efekt datapoolu za současného přihlédnutí k počtu takto sdílených patentů. Bylo by totiž nanejvýš pošetilé vyhodnocovat dohodu v rámci datapoolu jako zakázanou v případě, kdy by následkem chyby chránila mezi stovkami platných patentů jeden neplatný.

Ná závěr pro úplnost zmiňme, že TTBER a na ní navazující pokyny se rovněž neaplikují v situacích kdy určí pro specifické případy jinak blokové výjimky[197] obsažené v nařízeních SBER[198] a R&D BER.[199]

5.1.1.4 Sdílení informací za účelem výzkumu a vývoje

Další bloková výjimka podle odst. 3 článku 101 SFEU je výjimka dopadající na datapooly vytvářené za účelem sdílení poznatků ohledně výzkumu a

---

[196] Odstavce 272 a 128 sdělení komise k Nařízení Komise (EU) 316/2014 ze dne 21. března 2014 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie dohod o převodu technologií ve spojení s čl. 5 Nařízení Komise (EU) 316/2014 ze dne 21. března 2014 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie dohod o převodu technologií písmeno b), datapool by zde totiž mohl fakticky působit jako závazek nenapadnout práva duševního vlastnictví. Viz. Sdělení Komise Pokyny o použití článku 101 Smlouvy o fungování Evropské unie na dohody o převodu Technologií.

[197] Odstavec 7 preambule Nařízení Komise (EU) 316/2014 ze dne 21. března 2014 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie dohod o převodu technologií

[198]Nařízení Komise (EU) 2023/1067ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie specializačních dohod

[199] Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

vývoje. Pro účely moderních datapoolů je tato kategorie naprosto stěžejní a podporuje tak vlastně konkurenceschopnost a udržitelnost celé Evropské unie.

Pravidlo obsažené v této blokové výjimce se aplikuje na DSA, které by jinak spadaly do oblasti zakázaných za podmínky, že jsou předmětem sdílení data o výzkum a vývoji technologií nutných pro výrobě výrobků, vyráběných stranami. Tato data musí být tajná, podstatná a identifikovatelná.[200] Což znamená, že aby bylo možné na sdílení dat výjimku aplikovat, musí být data užitečná a důležitá pro produkční aktivity[201] stran a nebo užití určitého předem stanoveného okruhu technologií. Zmíněná data musí být rovněž přístupná pouze určitému okruhu uživatelů vymezenému v DSA. Pokud by se tak nestalo a data byla přístupná všem, neaplikoval by se článek 101 SFEU a nebyl by tudíž ani důvod k užití blokové výjimky.

V zásadě přitom platí, že aby byla bloková výjimka aplikovatelný musí mít strany DSA rovný a kompletní přístup k veškerým[202] výsledkům výzkumu a vývoje sdíleným podle této dohody. Je rovněž nutné aby byla data publikována bez zbytečných průtahů, hned poté co jsou spolehlivě získána.[203] Případná prodleva mezi získáním dat a jejich zveřejněním by totiž mohla představovat nespravedlivou konkurenční výhodu.

Pokud dochází při výzkumu a vývoji k určité disproporcionalitě mezi stranami, například určitá společnosti mají větší R&D oddělení než jiné a nebo některé společnosti přispívají do datapoolu pouze daty potřebnými pro další výzkum a vývoj, zatímco jiné data i aktivně zpracovávají, je přípustné aby si strany ujednaly jistou finanční částku, která spravedlivě vynahradí tuto disproporci. Tato částka ale nesmí být v takové výši, aby bránila stranám v přístupu k tomuto know-how. Fakultativně je rovněž možné, aby si strany mezi sebou ujednaly společné zadání výzkumu za finanční úplatu, kdy bude sdílení nákladů a výsledků z kontraktace specializovaného pracoviště benefitem pro všechny zúčastněné a umožní přístup k výsledkům a jejich využití. Strany rovněž

---

[200] Článek 1 odst. 9 Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

[201] produkován může být výrobek a nebo služba.

[202] Článek 3 odst. 3 písmeno a) Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

[203] Ibid. článek 3 odstavec 3 písmeno b)

musí mít přístup k veškerému dosavadnímu know how, které je potřebné pro využití dat o výzkumu a vývoji sdílených v datapoolu.[204]

Pokud však mezi sebou vytvářejí datapool akademické instituce, nebo společnosti jejichž hlavní činností je provádění výzkumu na komerční bázi, mohou si mezi sebou ujednat, že budou používat data na sdílená v datapoolu pouze pro účely budoucího výzkumu a vývoje.[205]

Výše zmíněné případy spadající do výjimek podle R&D BER, jsou omezené co se týče rozsahu a doby na kterou je dohoda uzavírána. Bloková výjimka se na tyto datapooly uplatní, pokud je datapool vytvořen mezi konkurenčními společnostmi, které zaujímají na relevantních trzích výrobků a technologií ne více, než 25%.[206] Podíly na trhu jsou stanovovány na základě hodnot prodejů za předchozí relevantní kalendářní rok. Výjimka obsažená R&D BERse rovněž neuplatní pokud je součástí dohody o vytvoření cloudu omezení, zakazující paralelní nezávislý výzkum v jiných oblastech nesouvisejících s dohodou a nebo pokud se v DSA zakládající cloud nacházejí tvrdá omezení soutěže jako je omezení výroby, prodeje nebo vývozu, omezení území na kterém smí strany pasivně prodávat atd.[207]

Jako v případě všech blokových výjimek může být i tato výjimka odejmuta Komisí či orgánem pro ochranu hospodářské soutěže členského státu, za předpokladu, že je v konkrétním případě zjištěno, že datapool obsahující data sdílená na základě ujednání o společném výzkumu a vývoji, působí převážně protisoutěžně.

Vice versa však fakt, že datapool nespadá do blokové výjimky R&D BER například z důvodu procent jež zaujímají jeho zakladatelé na relevantním trhu, neznamená, že se jedná automaticky o zakázané protisoutěžní ujednání podle článku 101 odst. 1 SFEU. Takovýto datapool stále může splnit obecné podmínky odst. 3 výše zmíněného článku.

---

[204] Odůvodnění Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

[205] Článek 3 odst. 5 Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

[206] Článek 6 Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

[207] I z tohoto pravidla však existují specifické výjimky blíže článek 8 Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

5.1.1.5 Sdílení informací za účelem koordinace specializace

Datapooly obsahující specializační dohodu budou spíše okrajovým fenoménem, nicméně i tak mohou hrát v určitých případech nezastupitelnou roli z hlediska ekonomiky Unie a proto jim bude alespoň stručně věnována pozornost i zde. Typickým příkladem specializačních dohod v oblasti datapoolingu budou zejména dohody o společné přípravě určitých služeb. K vytváření takovýchto datapoolů mezi společnostmi dochází převážně v momentech kdy každá že společností již má jistý trh či oblast trhu na které s úspěchem působí, vlivem okolností se však rozhodne spojit síly s jinou společností za účelem rozšíření prodeje či výroby svých výrobků a nebo poskytování služeb. A to buď geograficky a nebo prostřednictvím rozšířením produktového portfolia. V takovémto případě společnost nemá zájem slučovat svůj systém se systémem smluvního partnera a proto vytvoří nový sdílený datapool pro sdílení dat potřebných k relevantnímu účelu, který je sdílen a dalšími subjekty jichž se ujednání týká.

Současná právní úprava pak rozeznává tři druhy specializačních dohod. A sice specializační dohody jednostranné ve kterých se jedna strana zavazuje k omezení svých podnikatelských aktivit ve prospěch strany druhé, specializační dohody reciproční, ve kterých se strany vzájemně zavazují omezit či zastavit podnikatelské aktivity v určitém oboru výměnou za omezení či zastavení podnikatelských aktivit druhé strany v oboru jiném a nebo dohody, ve kterých se strany zavazují vyrábět určitý výrobek společně.[208] Role datapoolů bude silná zejména ve třetím zmiňovaném případě, kdy si budou společnosti pomocí technologického datapoolu v reálném čase sdílet informace a licence nutné pro efektivní výrobu.

Na výše zmíněné dohody se tedy uplatní bloková výjimka SBER[209], ovšem za předpokladu, že podíl stran datapoolu uzavírajících dohodu o koordinaci a specializaci nepřekročí na relevantním výrobkovém trhu 20%. Tato bloková výjimka však může samozřejmě být odejmuta Komisí a nebo orgánem pro ochranu hospodářské soutěže členského státu.

Na závěr této kapitoly, je vhodné pro úplnost zmínit, že určitá pravidla týkající se hospodářské soutěže se mohou rovněž mohou dopadat na datapooly

---

[208]Nařízení Komise (EU) 2023/1067 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie specializačních dohod. Článek 5.

[209] Nařízení Komise (EU) 2023/1067 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie specializačních dohod

prostřednictvím omezení poskytovatelů cloud computing služeb v režimu tzv. strážců přístupu v režimu nařízení DMA[210] s to souladu s odstavcem 1 a odstavcem 2 písmeno i) článku 2 tohoto nařízení.

6. Závěr

Cílem předkládané práce bylo přiblížit právní aspekty techniky datapooling v současném evropském právu. Vzhledem k tomu, že oblast moderních technik v IT je vzhledem k rychlému a dynamickému vývoji tohoto oboru dlouhodobě legislativně nedostatečně upravená, zaměřila se autorka na hledání možných východisek v interpretaci jednotlivých obecných legislativních zdrojů a hledání bezpečných cest rozvoje tohoto odvětví s ohledem na předpokládaný vývoj.

Jako největší problém ve vztahu práva a datapoolingu autorka spatřuje nedostatečnou edukaci generace současných právníků ve vztahu k IT právu. Výše nastíněná situace se přitom, vzhledem k absenci povinné kvalitní výuky IT práva na většině evropských univerzit v dohledné době nezlepší. Dalším nezanedbatelným problémem je pak rigidní přístup některých odborníků, kteří se snaží k tomuto právnímu odvětví přistupovat stejně, jako k právním odvětvím poněkud konvenčnějšího rázu, s tím, že se na problémy IT práva snaží, poněkud nešťastně, aplikovat vzorce z občanského práva, s tím, že očekávají, že se tomu společnosti i jednotlivci působící v IT přizpůsobí. Tento přístup je však poněkud problematický, čisté z toho důvodu, že tak mnohdy právo popírá základní matematické a technologické zákonitosti.

Hlavní krátkodobá východiska v oblasti datapoolingu lze přitom nalézt v oblasti smluvní, ve které mohou strany, při kvalitní spolupráci odborníků z oblasti práva a IT, stanovit podmínky, které mohou pomoci překlenout legislativní deficit. Kvalitní spolupráce IT odborníků a právníků při vytváření smluvních základů datapoolů pak může i vytvořit obecně uznávaná standard, ze kterého může postupně vyjít národní i nadnárodní regulace, která převezme to nejlepší z praxe, místo toho, aby vytvářela vlastní systém metodou pokus-omyl.

Věrna výše zmíněnému autorka v první části práce alespoň v hrubých rysech nastínila základní technologie používané v oblasti datapoolingu, společně s právními problémy, které tyto technologie skýtají, spolu s nastíněným možných

[210] Odstavec 7 odůvodnění DMA

řešení, případně alespoň způsobů kterými lze v závislosti na specifících jednotlivých datapoolů hledat řešení. V druhé a třetí části pak autorka rozebrala náležitosti ochrany dat, a to osobních i neosobních. Akcentovala zde rovněž postavení dat v soudobé společnosti, jakožto aktiva sui generis. S ohledem na to se pak autorka v maximální míře soustředila na nalézání právně, ekonomicky i eticky udržitelných řešení. V poslední části práce se pak autorka věnovala vymezení pozice datapoolingu z pohledu efektu na hospodářskou soutěž a její právní úpravu.

Co se týče návrhu na zlepšení, lze vzhledem k technickým a organizačním možnostem zákonodárce pouze navrhnout aby byla do budoucna přijata taková opatření, která budou lépe zohledňovat fungování ICT, a to zejména s tím, že budou normovat spíše prostředky jakými má být dosaženo výsledku nežli výsledek jako takový. Bude vhodné, aby při přípravě jakékoliv regulace bylo přihlíženo k již praxí zavedeným postupům a standardům, neboť je možno očekávat, že chybné koncepty zanikly a darwinisticky přežily nejsilnější koncepty a optimální řešení. Autorka rovněž uvítá vyjasnění charakteru dat zejména z pohledu jejich možného vnímání spíše jako věci nehmotné, nežli jako informace.

Nebývá zvykem zakončovat vědecké práce prosbou. V tomto případě by však autorka ráda udělala výjimku a poprosila laskavého čtenáře, aby shlédl na IT právo a datapooling okem milostivým, a i přes jeho velký přesah do světa technologií se pokusil najít v tomto odvětví práva zalíbení. Nemusí při tom hned dávat přihlášku na některý z technologických oborů, byť entusiasmu se samozřejmě meze nekladou. Bohatě postačí, když si vybere jeho srdci blízký druh lidské činnosti a zamyslí se, jakým způsobem se vlivem ICT změnil a jaké jsou v tomto směru další možnosti jeho rozvíjení. Jak praví citát připisovaný Albertu Einsteinovi: „*Žádný problém nemůže být vyřešen na stejné úrovni myšlení, která jej stvořila*.“

Resumé

The master's thesis titled "Legal Aspects of Datapooling in the European Union" delves into the subject of datapooling through the lens of European Union law, which stands as a trailblazer in the legal regulation of this emerging legal domain.

Structured with an introduction, conclusion, and four principal sections, the thesis navigates various facets of datapooling.

In the initial section, the author elucidates datapooling as a technique, scrutinizes its rationale, explores conceivable approaches to constructing a datapool, and underscores pivotal considerations that must be addressed by designers in this realm.

The subsequent section delves into the realm of personal data protection, delineating the essence of informed consent, dissecting its constituent elements, and elaborating on the status and responsibilities of the data controller, as well as the processing and safeguarding of personal data, all within the purview of European Union legislation and established jurisprudence.

The third segment is dedicated to an often-neglected subject: the protection of non-personal data, an area overshadowed by the more prominently discussed protection of personal data.The fourth section of this study is dedicated to the safeguarding of competition, wherein the author deliberates on the potency of datapool technology and its ramifications on the outcomes of individual market participants. The author elucidates that a meticulously crafted datapool confers a competitive edge upon its users vis-à-vis their rivals and can wield substantial influence on competition dynamics. An examination is undertaken regarding the accessibility of datapools by various market competitors, juxtaposing the economic benefits to consumers derived from the enhanced efficiency of suppliers and their augmented profitability against the adverse impact on the market position of other suppliers. This analysis underscores that in conditions fostering positive consumer effects and equitable competition, datapool emerges as yet another instrument of evolutionary selection in a liberated and transparent market. Neglecting its significance poses a palpable risk to competitive integrity.

In light of the transnational significance of datapools, this paper predominantly relies on legislation and jurisprudence established at the European Union level. Its findings are applicable, albeit with discretion, across EU Member States, recognizing that national legislation may exhibit stringency on certain matters while remaining aligned with the foundational principles of EU law.

Seznam použitých zdrojů

Právní předpisy

Bernská úmluva o ochraně literárních a uměleckých děl ze dne 9. září 1886, Doplněná v Paříži dne 4. května 1896, revidovaná v Berlíně dne 13. listopadu 1908, doplněná v Bernu dne 20. března 1914, a revidovaná v Římě dne 2. června 1928, v Bruselu dne 26. června 1948, ve Stockholmu dne 14. července 1967 a v Paříži dne 24. července 1971

Code of Federal Regulations

Evropská úmluva o ochraně lidských práv. Online. Dostupné z: https://www.echr.coe.int/documents/d/echr/convention_ces

Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) - GDPR

Nařízení Komise (EU) 2022/720 ze dne 10. května 2022 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie vertikálních dohod a jednání ve vzájemné shodě

Nařízení Komise (EU) 316/2014 ze dne 21. března 2014 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na kategorie dohod o převodu technologií

Nařízení Komise (EU) 2023/1066 ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie dohod o výzkumu a vývoji

Nařízení Komise (EU) 2023/1067ze dne 1. června 2023 o použití čl. 101 odst. 3 Smlouvy o fungování Evropské unie na některé kategorie specializačních dohod

Modernizovaná úmluva 108+ vydaná Radou. Evropy Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [Citováno 31. března 2024]

Směrnice Rady 93/13/EHS ze dne 5. dubna 1993 o nepřiměřených podmínkách ve spotřebitelských smlouvách

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází

Směrnice Evropského parlamentu a 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů

Zákon Spojeného království o ochraně dat z roku 1998. Online. Dostupné z: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted

WORLD INTELLECTUAL PROPERTY ORGANIZATION. WIPO PUBLICATION No. 464 (E) -IMPLICATIONS OF THE TRIPS AGREEMENT ON TREATIES ADMINISTERED BY WIPO. Přetisk 2012. ISBN 978-92-805-0681-1

Judikatura

Rozsudek pátého senátu Soudního dvora Evropské unie ze dne 19. listopadu 1998 ve věci Nilsson and others, C-162/97, ECLI:EU:C:1998:554

Rozsudek čtvrtého senátu Soudního dvora Evropské unie ze dne 22. listopadu 2008 ve věci Friederike Wallentin-Hermann, C-549/07, ECLI:EU:C:2008:771

Rozsudek šestého senátu Soudního dvora Evropské unie ze dne 9. února 1995 ve věci Leclerc-Siplec v TF1 and M6, C-412/93, ECLI:EU:C:1995:26

Rozsudek prvního senátu Soudního dvora Evropské unie ze dne 12. ledna 2023 ve věci Österreichische Post (Informations relatives aux destinataires de données personnelles), C-154/2, ECLI:EU:C:2023:3

Rozsudek Velkého senátu Soudního dvora Evropské unie ze dne 5. června 2018 ve věci Wirtschaftsakademie Schleswig-Holstein, C-210/16, ECLI:EU:C:2018:388

Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 18. září 2001 ve věci M6 and Others v Commission, T-112/99, ECLI:EU:T:2001:215

Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 6. října 2006 ve věci GlaxoSmithKline Services and Others v Commission and Others, C-501/06 P, ECLI:EU:C:2009:610

Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 8 července 2008 ve věci AC-Treuhand v Commission, T-99/04, ECLI:EU:T:2008:256

Rozsudek třetího senátu Soudního dvora Evropské unie ze dne 11 září 2014 ve věci CB v Commission, C-67/13 P, ECLI:EU:C:2014:2204

Rozsudek pátého senátu Soudního dvora Evropské unie ze dne 28. května 1998 ve věci John Deere Ltd. v Commission, C-7/95 P. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61995CJ0007

Rozsudek Soudního dvora Evropské unie ze dne 25. října 1977 ve věci Metro v Commission, C-26/76, ECLI:EU:C:1977:167

Publikace

Christopher, BYGRAVE, Lee, DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU General Data Protection Regulation (GDPR); A Commentary*. Oxford University Press, 2020. ISBN 978–0–19–882649–1.

MILLARD, Christopher. *Cloud Computing Law*. Oxford University Press, 2013. ISBN 978–0–19–967168–7.

KELLERBAUER, Manuel; KLAMERT, Marcus a TOMKIN, Johnathan (ed.). T*he EU Treaties and the Charter of Fundamental Rights. A Commentary*. Oxford university press, 2019. ISBN 978–0–19–879456–1.

RABAN, Přemysl, a kol. *Obchodní právo*. Brno. Václav Klemm - Vydavatelství a nakladatelství, 2020. ISBN 978-80-87713-19-8

Odborné články

DAM, Tobias, Maxmilian HENZL, Lukas Daniel KLAUSNER, *Delete My Account: Impact of Data Deletion on Machine Learning Classifiers*. Online. ArXiv 2023. Dostupné z: https://doi.org/10.48550/arXiv.2311.10385

FLORIDI, Luciano, Carl ÖHMAN. *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*. Online. Minds & Machines vol. 27 z roku 2017, str. 639–662. https://doi.org/10.1007/s11023-017-9445-2

NAKAGAWA, Hiroshi, Akiko ORITA. *Using deceased people's personal data*. Online. AI & Society, z roku 2022. https://doi.org/10.1007/s00146-022-01549-1

POLČÁK, *Radim*. *Informace a data v právu*. Revue pro právo a technologie. Roč. 2013, č. 13. ISSN 1805-2797.

VAN DE WAERDT, Peter. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Business Horizons vol. 4 roku 2023. Strany 493 - 504. Dostupné z: doi:https://doi.org/10.1016/j.bushor.2022.10.002

SCHÄFER, Fabian, Heiko GEBAUER, Christoph GRÖGER, Oliver GASSMANN a Felix WORTMANN. Data-driven business and data privacy: Challenges and measures for product-based companies. Computer Law & Security Review vol. 38 z roku 2020. ISSN 0267-3649. Dostupné z: doi:https://doi.org/10.1016/j.clsr.2020.105436

WANG, Shangping, Yinglong ZHANG, Yaling ZHANG. A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. IEEE Xplore, vol. 6, z roku 2018. ISSN: 2169-3536 pp. 38437-38450. Dostupné z: http://dx.doi.org/10.1109/ACCESS.2018.2851611

Online zdroje

AWS Customer Agreement ve verzi z 27. října 2023 odstavec 2.2. Online. Dostupné z https://aws.amazon.com/agreement/ - [cit. 2023-4-11]

Cloudové výpočetní úložiště aneb kapacita i výkon na jednom místě. Online. In: www.cestadocloudu.cz. Dostupné z: https://www.cestadocloudu.cz/blog/cloudove-vypocetni-uloziste-aneb-kapacita-i-vykon-na-jednom-miste/. [cit. 2023-08-08]

COMMPORT, Online. Dostupné z : https://www.commport.com/global_data_synchronization_network/ [citováno dne 11.11.2023]

EVROPSKÁ KOMISE. *European data strategy: Making the EU a role model for a society empowered by data*. *Online*. Dostupné z: https://

commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. [cit. 2024-03-30].

Cloud Terms and conditions Online. Dostupné z: https://www.apple.com/legal/internet-services/icloud/cz/terms.html [cit. 2023-5-11]

LEXOLOGY. When is data pooling anticompetitive? Online. Dostupné z: https://www.lexology.com/library/detail.aspx?g=40bb6970-8419-4f78-90aa-a9e160c61ef7. [cit. 2024-03-30]

MICROSOFT CORPORATION INC. *Co je PaaS? Platforma jako služba*. Online. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-paas. [cit. 2024-03-31].

How do we do a DPIA? Online. Dostupné z: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how12. [cit. 2024-03-31].

OECD. *Data-Driven Innovation: Big Data for Growth and Well-Being*. Online. OECD Publishing, 2015. https://doi.org/10.1787/9789264229358-en. [cit. 2024-03-30]

POOL blíže stránky společnosti: https://www.pooldata.io/about-us [citováno dne 11.11.2023]

Pokyny pro souhlas podle nařízení 2016/679 přijaté dne 28. listopadu 2017 v revidovaném znění přijatém dne 10. dubna 2018 Pracovní skupinou zřízenou podle článku 29. Online. Dostupné z: https://www.ipvz.cz/seznam-souboru/4864-pokyny-pro-souhlas-podle-narizeni-vystaveno-dne-14-03-19.pdf [Citováno 30. března 2024]

Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR Verze 2.0 přijaté dne 7. července 2021 přijaté EDPB Dostupné z: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/

guidelines-072020-concepts-controller-and-processor-gdpr_en [Citováno 30. března 2024]

Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 4. října 2017 v aktualizovaném znění Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Dostupné z: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/vysoke-riziko.pdf [Citováno 30. března 2024]

Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 přijaté dne 3. října 2017, ve znění naposledy revidovaném a přijatém dne 6. února 2018 Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Dostupné z: https://ec.europa.eu/newsroom/article29/items/612053 [Citováno 30. března 2024]

Pokyny k funkci pověřence pro ochranu osobních údajů schválené dne 13. prosince 2016 Pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Neoficiální překlad dostupný z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2018/1/Preklad-Metodiky-poverence-WP29.pdf.[Citováno 30. března 2024]

Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci 14. ledna 2011 Komisí. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52011XC0114(04). [Citováno 30. března 2024]

SaaS, PaaS & IaaS Agreements Lawyers & Attorneys. Online. Dostupné https://www.priorilegal.com/contracts/saas-paas-and-iaas-agreements z: [cit. 2024-03-31].

Sdělení Komise Pokyny o použití článku 101 Smlouvy o fungování Evropské unie na dohody o převodu Technologií. Online. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52014XC0328(01). [Citováno 31. března 2024]

Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů s názvem Směrem ke společnému datovému prostoru ze dne 25. dubna 2018. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0232

Stanovisko Evropského inspektora ochrany údajů č. 3/2018 o online manipulaci a osobních datech, strana 8. Dostupné z https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf [Citováno 5. února 2024]

SZABO, Nick. *Smart Contracts*. Online. Dostupné z: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. [Citováno 22. března 2024]

The DPIA Process - a step-by-step guide. Online. Dostupné z: https://www.lboro.ac.uk/data-privacy/resources/dpia/dpia-process. [cit. 2024-03-31]