



Český telekomunikační úřad

Průvodce ČTÚ nařízením DSA

pro uživatele služeb

Verze 31. 10. 2024

Zpracováno ve spolupráci
s Úřadem pro ochranu osobních údajů
a Ministerstvem průmyslu a obchodu



Úřad pro ochranu
osobních údajů



MINISTERSTVO
PRŮMYSLU A OBCHODU

Obsah

1.	Úvod	2
2.	Pro koho je tento Průvodce určen?	3
3.	Přehled hlavních přínosů nařízení DSA pro uživatele	3
4.	U jakých poskytovatelů lze uplatnit práva dle nařízení DSA?	3
5.	Jaká mají uživatelé práva dle nařízení DSA vůči poskytovatelům a jak je mohou uplatnit?	6
6.	Transparentnost poskytovatelů služeb	7
6.1.	Kontaktní místo	6
6.2.	Právo komunikovat s člověkem	7
6.3.	Pravidla pro smluvní podmínky	7
6.4.	Zprávy o transparentnosti	8
6.5.	Databáze transparentnosti	8
6.6.	Transparentnost doporučovacích systémů	8
6.7.	Archiv reklam	9
7.	Pravidla moderace obsahu	9
7.1.	Oznamování nezákonného obsahu	9
7.2.	Odůvodnění omezení	11
7.3.	Interní systém vyřizování stížností	13
7.4.	Systém mimosoudního řešení sporů	13
8.	Ochrana uživatelů online platform	14
8.1.	Zákaz dark patterns	14
8.2.	Ochrana nezletilých osob	15
8.3.	Regulace online reklamy	16
8.4.	Ochrana spotřebitelů na online tržištích	17
8.5.	Ochrana před systémovými riziky	18
9.	Dozor nad dodržováním povinností	19
10.	Jak podat stížnost	19
11.	Právo uživatelů na náhradu škody	20
12.	Další zdroje	21

1. Úvod

Ústava pro internet nebo konec digitálního divokého západu. I taková označení jsou přisuzována [nařízením Evropského parlamentu a Rady \(EU\) 2022/2065 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES](#) (dále jen „nařízení DSA“), které nabylo účinnosti dne **17. února 2024**. Jedná se o komplexní právní předpis, který zavádí v celé Evropské unii **jednotná pravidla pro poskytovatele digitálních zprostředkovatelských služeb** s cílem vytvořit bezpečné, předvídatelné a důvěryhodné online prostředí, ve kterém se daří inovacím a v němž jsou zároveň účinně chráněna základní práva. Těchto cílů má dosáhnout především nastavením nových povinností pro poskytovatele služeb. Příjemcům služeb nařízení DSA naopak přiznává nová práva, díky kterým mají větší kontrolu nad poskytovanými službami.

Hlavními cíli nařízení DSA jsou:

- Posílení práv příjemců služeb,
- Podpora transparentnosti,
- Regulace velkých online platforem,
- Zavedení opatření proti nezákonnému obsahu a systémovým rizikům,
- Zapojení občanské společnosti do uplatňování a vymáhání pravidel.

V České republice bude na nařízení DSA navazovat [zákon o digitální ekonomice](#), který se nyní nachází v legislativním procesu a který mimo jiné stanoví působnost orgánů veřejné správy odpovědných za kontrolu povinností dle nařízení DSA a odpovědnost za přestupky spočívající v porušení tohoto nařízení. Nařízení DSA ukládá členským státům, aby určily **koordinátora digitálních služeb**, jakožto nezávislý a nestranný orgán, který bude dohlížet na dodržování povinností podle nařízení DSA ze strany subjektů sídlících v daném členském státě. V České republice byl tímto úkolem pověřen **Český telekomunikační úřad** (dále jen „Úřad“ nebo „ČTÚ“). Vedle něj bude dozor v záležitostech online reklamy vykonávat Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“).

Úřad zastává názor, že je důležité veřejnosti pomoci s porozuměním pravidlům podle nařízení DSA a poskytnout jí jejich srozumitelný výklad. Je nutné zdůraznit, že tento Průvodce je právně nezávaznou pomůckou. Pro posouzení reálných podnětů bude vždy nutné vzít do úvahy okolnosti konkrétního případu. **Úřad rovněž není oprávněn rozhodovat spory mezi poskytovateli a jejich uživateli ani nařizovat odstranění nezákonného obsahu.** Dále je nutné zmínit, že nařízením DSA není dotčeno dodržování jiných vnitrostátních či evropských právních předpisů, jako jsou nařízení GDPR¹, DMA² a P2B³ nebo předpisy o ochraně spotřebitele či relevantní ustanovení občanského zákoníku.

Pro úplnost dodáváme, že veškeré příklady uvedené v tomto průvodci jsou pouze ilustrativní. Příklady předpokládají, že poskytovatelé, uvedení v jednotlivých příkladech jsou pro účely tohoto průvodce povinnými osobami ve smyslu příslušného ustanovení nařízení DSA, skutečné hodnocení aplikovatelnosti nařízení DSA na takové poskytovatele však vždy závisí na konkrétních okolnostech.

Pro odpovědi na další otázky spojené s nařízením DSA kontaktujte ČTÚ na e-mailové adrese podatelna@ctu.cz.

¹ Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

² Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích)

³ Nařízení Evropského parlamentu a Rady (EU) 2019/1150 o podpoře spravedlnosti a transparentnosti pro podnikatelské uživatele online zprostředkovatelských služeb.

2. Pro koho je tento průvodce určen?

Tento průvodce je určen všem uživatelům, resp. příjemcům služeb, kteří se nacházejí nebo jsou usazeni v EU a kteří využívají zprostředkovatelské služby podle nařízení DSA bez ohledu na to, zda jsou spotřebiteli či podnikateli, fyzickými či právníckými osobami nebo jednájí jménem orgánu veřejné moci.

3. Přehled hlavních přínosů nařízení DSA pro uživatele

Transparentnost poskytovatelů služeb

- Kontaktní místo
- Právo komunikovat s člověkem
- Pravidla pro smluvní podmínky
- Zprávy o transparentnosti
- Databáze transparentnosti
- Transparentnost doporučovacích systémů
- Archiv reklam

Ochrana uživatelů online platform

- Zákaz dark patterns
- Ochrana nezletilých osob
- Regulace online reklamy
- Ochrana spotřebitelů na online tržištích
- Zmírňování systémových rizik



Pravidla moderace obsahu

- Oznamování nezákonného obsahu
- Odůvodnění omezení
- Interní systém vyřizování stížností
- Mimosoudní řešení sporů

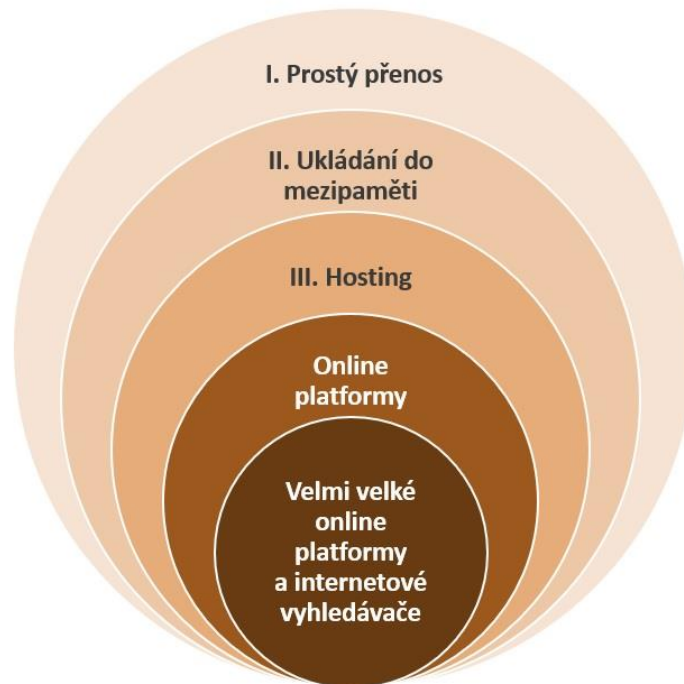


4. U jakých poskytovatelů lze uplatnit práva dle nařízení DSA?

Nařízení DSA nereguluje celý internet, ale jen tu část, která využívá uživatelský obsah. Je tedy závazné pro všechny **poskytovatele zprostředkovatelských služeb**, kteří nabízejí své služby příjemcům, kteří jsou usazeni nebo se nacházejí na území EU. ČTÚ zdůrazňuje, že **nařízení DSA neukládá žádné povinnosti uživatelům služeb**.

Poskytovaná zprostředkovatelská služba musí být tzv. **službou informační společnosti** dle směrnice (EU) 2015/1535, která je definována jako služba poskytovaná **na dálku, elektronicky, na individuální žádost příjemce a zpravidla za úplatu (více informací o kritériích služby informační společnosti naleznete v Průvodci ČTÚ k aplikaci nařízení DSA pro poskytovatele služeb**.

Nařízení DSA upravuje poskytování těch služeb informační společnosti, které lze zařadit mezi tři základní typy zprostředkovatelských služeb, a to **služby prostého přenosu, ukládání do mezipaměti a hosting**. Specifickou zprostředkovatelskou službou podle nařízení DSA jsou dále **internetové vyhledávače**.



a) Služby prostého přenosu

Prostý přenos = služba, která spočívá v přenosu informací poskytnutých příjemcem služby komunikační sítě nebo v poskytování přístupu ke komunikační síti. V rámci této služby dochází ke krátkodobému ukládání přenášených informací, nicméně pouze po dobu nutnou k uskutečnění přenosu. Poskytovateli prostého přenosu jsou např.:

- poskytovatelé připojení k internetu,
- poskytovatelé otevřené Wi-Fi sítě,
- služby instant messagingu (tedy služby sloužící pro komunikaci v reálném čase, nicméně část jejich služeb je možné považovat též za hosting),
- centralizované peer to peer sítě,
- virtuální privátní sítě,
- přenosové mobilní služby,
- přenos mezi sítěmi,
- výměnné uzly internetu,
- služby a resolversy systému doménových jmen,
- registry názvů domén nejvyšší úrovně,
- webové prohlížeče,
- platformy pro videohovory apod.

b) Ukládání do mezipaměti (caching)

Ukládání do mezipaměti (caching) = služba zahrnující kromě přenosu informací také dočasné ukládání informací, avšak pouze pro účelnější nebo bezpečnější přenos dat, ke kterému může dojít na žádost jiného příjemce služby. Zjednodušeně řečeno je skrz tuto službu vytvořena kopie dat za účelem rychlejšího přístupu k nim pro jiné uživatele. V praxi je tato služba využívána např. k rozložení komunikační zátěže, kdy se krátkodobá kopie dat uloží na serveru, který je pro uživatele geograficky blíže než server původní. Příklady cachingu zahrnují:

- poskytování sítí pro doručování obsahu,
- provoz cachovacích serverů,
- reverzní proxy služby,
- proxy služby k úpravě obsahu,
- systémy ochrany proti DDoS útokům apod.

c) Hosting

Hosting – Služba, která umožňuje uživatelům na jejich žádost ukládat informace. Hosting tedy nelze vnímat pouze úzkou optikou webhostingu, mimo něj sem spadají např.:

- diskuzní fóra,
- internetové aukční portály,
- služby umožňující přidávání recenzí,
- datová úložiště souborů,
- cloudová úložiště,
- herní servery,
- cestovní a bytovací platformy,
- platformy sdílené ekonomiky,
- sociální sítě,
- komunitní platformy,
- instant messaging (tedy služby sloužící pro komunikaci v reálném čase, nicméně část jejich služeb je možné považovat též za prostý přenos) apod.

d) Online platformy

Podkategorií hostingu je **Online platforma** – jedná se o hostingovou službu, která krom toho, že příjemci služby umožňuje uložení informace, umožňuje navíc také **na žádost příjemce služby** veřejné šíření takto uložené informace. Veřejným šířením se rozumí zpřístupňování informací na žádost příjemce služby, který informace poskytl, potencionálně neomezenému počtu třetích stran. O online platformu se však nejedná, pokud je tato činnost **nepodstatným a pouze pomocným prvkem jiné služby nebo nepodstatnou funkcí hlavní služby** jako např. sekce komentářů v rámci internetových novin nebo poskytování prostoru pro online reklamu na internetové stránce. Příklady online platform jsou:

- sociální sítě,
- **online tržiště** (k definici online tržiště viz bod e) níže),
- diskuzní fóra,
- internetové aukční portály,
- platformy pro sdílení videí,
- platformy pro sdílení souborů apod.

e) Online tržiště

Podkategorií online platform jsou **Online tržiště** – jedná se o online platformy umožňující spotřebitelům uzavírat s obchodníky smlouvy na dálku. Zvláštní povinnosti podle nařízení DSA tedy dopadají pouze na ta online tržiště, která umožňují uzavírání smluv mezi obchodníky a spotřebiteli (B2C). Další podmínkou je, že online tržiště musí umožňovat přímé uzavření smlouvy mezi stranami, nepostačí tedy pouze možnost zveřejnění nabídky a kontaktních údajů dané osoby. Pravidla pro online tržiště podle nařízení DSA proto nedopadají např. na některé inzertní portály nebo tržiště určená výhradně pro obchodní profesionály.

f) Internetové vyhledávače

Poslední kategorií služeb informační společnosti, o které hovoří nařízení DSA, jsou **Internetové vyhledávače** – jde o zprostředkovatelskou službu, která uživatelům **umožňuje vkládat dotazy za účelem vyhledávání** v zásadě na všech internetových stránkách v určitém jazyce na základě dotazu a **kteřá poskytuje výsledky v jakémkoli formátu, v nichž lze nalézt informace související s požadovaným obsahem**. Za internetové vyhledávače dle nařízení DSA naopak nelze považovat tzv. **vertikální vyhledávače**, tj. vyhledávače, které provádí specializované vyhledávání v rámci konkrétního oboru nebo tématu, např. nabízí pouze výsledky týkající se nabytí. Tyto vyhledávače však mohou být za určitých okolností hostingem nebo online platformou s doporučovacím systémem dle čl. 27 nařízení DSA.

g) Velmi velké online platformy a velmi velké internetové vyhledávače

Nad rámec výše uvedeného nařízení DSA definuje **Velmi velké online platformy a velmi velké internetové vyhledávače** – jedná se o takové online platformy a internetové vyhledávače, které mají průměrný měsíční počet aktivních uživatelů v Evropské unii nejméně **45 milionů**. O udělení tohoto statusu rozhoduje Evropská Komise. Mezi tyto subjekty aktuálně patří služby jako např. Facebook, LinkedIn, Instagram, YouTube nebo TikTok. Seznam všech subjektů spadajících do této kategorie je dostupný [zde](#). Na tyto služby se vztahují přísnější požadavky, na jejichž dodržování dohlíží přímo **Evropská komise**. Důležitým prvkem nařízení DSA je, že povinnosti poskytovatelům ukládá asymetrickým způsobem podle hesla „*s větší mocí přichází větší odpovědnost*“. Množství povinností, které musí poskytovatelé dodržovat je závislé na druhu poskytovaných služeb a velikosti podniku. Většina povinností proto cílí na střední a velké poskytovatele online platform, naopak vůči poskytovatelům prostého přenosu a [malým a mikro podnikům](#) se většina povinností neuplatní.

5. Jaká mají uživatelé práva dle nařízení DSA vůči poskytovatelům a jak je mohou uplatnit?

V následujících částech jsou popsána hlavní práva uživatelů podle nařízení DSA a s nimi související povinnosti poskytovatelů služeb.

6. Transparentnost poskytovatelů služeb

Jedním z hlavních cílů nařízení DSA je posílení transparentnosti evropského trhu digitálních služeb. Nastavení jasných a předem dostupných pravidel pro všechny aktéry a přístup veřejnosti k informacím o jejich uplatňování přispěje k zajištění spravedlivého a důvěryhodného online prostředí. Nařízení DSA tak významně posiluje schopnost uživatelů činit svobodná a informovaná rozhodnutí a v případě potřeby účinněji hájit svá práva.

6.1. Kontaktní místo

Všichni poskytovatelé služeb musí zřídit jednotné kontaktní místo pro své uživatele, prostřednictvím kterého je mohou uživatelé kontaktovat v případě potřeby. Kontaktní místo musí umožnit přímou, rychlou a uživatelsky vstřícnou komunikaci elektronickými prostředky, může mít podobu např. telefonního čísla, e-mailové adresy, kontaktního formuláře nebo chatovacího panelu. Informace nezbytné k tomu, aby mohli uživatelé kontaktní místa poskytovatelů snadno identifikovat a komunikovat s nimi, musí být snadno přístupné a průběžně aktualizované.

6.2. Právo komunikovat s člověkem

Každému uživateli musí být umožněno, aby si v rámci komunikace s kontaktním místem poskytovatele zvolil **možnost komunikovat s člověkem s vyloučením automatizovaných prostředků** jako jsou chatboty nebo umělá inteligence. Zejména při řešení specifických nebo složitějších problémů totiž nemusí být strojově navrhovaná řešení pro uživatele přínosem.

6.3. Pravidla pro smluvní podmínky

V minulosti mohli poskytovatelé stanovovat a uplatňovat pravidla fungování svých služeb takřka dle svého uvážení. Po účinnosti nařízení DSA musí každý poskytovatel uplatňující jakákoli omezení uživatelského obsahu **zveřejnit jasné, jednoznačné, srozumitelné, snadno pochopitelné a uživatelsky vstřícné smluvní podmínky**, tak aby se každý uživatel mohl předem seznámit se svými právy a povinnostmi předtím, než se rozhodne využít služeb poskytovatele. Tyto podmínky musí být veřejné a snadno dostupné. Velmi velké online platformy a velmi velké internetové vyhledávače musí navíc zveřejnit své **podmínky v češtině** a uživatelům poskytnout stručné, snadno přístupné a strojově čitelné **shrnutí smluvních podmínek, včetně dostupných nápravných opatření a mechanismů pro zjednání nápravy**, a to v jasném a jednoznačném znění. Transparentní smluvní podmínky tak chrání uživatele před nepředvídatelným chováním a diskriminací ze strany poskytovatelů.

a) Obsah smluvních podmínek

Smluvní podmínky musí obsahovat:

- **Informace o veškerých omezeních, která poskytovatelé uplatňují v souvislosti s využíváním jejich služby** s ohledem na obsah nahraný uživatelem včetně uvedení důvodů pro jejich uložení, např. pozastavení nebo smazání uživatelského účtu nebo omezení viditelnosti,
- **Informace o veškerých zásadách, postupech, opatřeních a nástrojích používaných za účelem moderování obsahu** včetně rozhodování založeného na algoritmech a možností lidského dohledu,
- Pravidla použití interního systému pro vyřizování stížností.

Ostatní záležitosti jsou nadále ponechány na smluvní volnosti stran nejsou-li regulovány jinými předpisy. Pokud je služba primárně zaměřena na nezletilé osoby, musí poskytovatel navíc vysvětlit podmínky této služby a jakákoli omezení jejího využívání způsobem, kterému nezletilé osoby rozumějí, tj. např. s využitím grafických prvků, informačních bannerů či krátkých videí.

b) Změna smluvních podmínek

Dále mají poskytovatelé povinnost uživatele **informovat o každé významné změně smluvních podmínek** např. e-mailem nebo zprávou v online rozhraní. Za významnou změnu se považují například situace, kdy poskytovatel mění pravidla týkající se informací, které jsou v rámci jejich služby povoleny, nebo jiné změny, které by mohly mít přímý dopad na schopnost příjemců službu využívat.

Při uplatňování a vymáhání smluvních podmínek jsou poskytovatelé povinni postupovat objektivně, přiměřeně a s náležitou péčí a patřičně přihlížet k právům a oprávněným zájmům všech dotčených stran včetně základních práv uživatelů, například svobody projevu, svobody a plurality médií a jiných základních práv a svobod obsažených Listině základních práv EU. Cílem je zabránit poskytovatelům ve svévolné aplikaci smluvních podmínek, která by vedla k diskriminaci nebo nepřiměřenému omezování základních práv uživatelů. Dle názoru ČTÚ např. není přípustné, aby poskytovatelé ukládali různým

uživatelům za totéž porušení smluvních podmínek odlišné omezení služeb, aby ukládali nepřiměřená omezení služeb nebo aby postihovali uživatele za jednání, které není zjevně v rozporu se zákonem ani smluvními podmínkami.

Příklad 1: Poskytovatel zájmového diskusního fóra pro zahrádkáře smazal příspěvek uživatele, který na tomto fóru inzeroval prodej svého osobního automobilu. Svůj postup poskytovatel odůvodnil ustanovením smluvních podmínek, podle něhož má správce právo odstranit příspěvky příjemců služeb, které nesouvisí se zahrádkářskou činností. Dotčený uživatel byl o opatření informován v souladu s čl. 17 nařízení DSA, přesto s rozhodnutím nesouhlasí s odkazem na svobodu projevu.

Vysvětlení: Poskytovatel postupoval v souladu s nařízením DSA. Poskytovatel si může ve svých podmínkách transparentně stanovit přiměřená pravidla omezující okruh témat, o kterých je možné diskutovat.

Příklad 2: Poskytovatel veřejného úložiště omezil viditelnost fotografie nahrané uživatelem. Tento krok odůvodnil ustanovením smluvních podmínek, podle kterého „může přijmout omezující opatření proti informaci poskytnuté příjemcem služby, pokud ji detekuje jeho interní systém na odhalování problematického obsahu“.

Vysvětlení: Poskytovatel porušil nařízení DSA, neboť ustanovení smluvních podmínek, ze kterého vycházel, není dostatečně konkrétní. Smluvní podmínky v daném případě nestanovují, z jakých důvodů může poskytovatel přijmout opatření ani charakter možných opatření. Uživatel tak nemohl předvídat, jak se poskytovatel zachová.

6.4. Zprávy o transparentnosti

Aby měla veřejnost transparentní přístup k souhrnným informacím o praktickém uplatňování postupů podle nařízení DSA ve vztahu ke konkrétním službám, musí poskytovatelé služeb (s výjimkou malých a mikro podniků) **alespoň jednou ročně** zveřejnit na svých internetových stránkách zprávu o veškeré moderaci obsahu, kterou prováděli v příslušném období. Zpráva musí být ve strojově čitelném formátu snadno přístupná, jednoznačná a snadno srozumitelná.

6.5. Databáze transparentnosti

Poskytovatelé online platforem (s výjimkou malých a mikro podniků) musí předkládat Evropské komisi bez zbytečného odkladu všechna rozhodnutí a odůvodnění, která jsou online platformy povinny poskytovat dle článku 17 odst. 1 nařízení DSA tak, aby mohly být zařazeny a zveřejněny v online [databázi transparentnosti](#), která slouží jako nástroj pro kontrolu a veřejný přístup k údajům o moderaci obsahu provádění poskytovateli online platforem.

Uživatelé a široká veřejnost tak má přístup k průběžným informacím o počtu a nejčastějších důvodech uložených omezujících opatřeních ze strany konkrétních platforem.

6.6. Transparentnost doporučovací systémů

Doporučovací systémy a algoritmy online platforem hrají zcela zásadní roli v tom, jaké informace a v jakém pořadí jsou příjemcům služeb prezentovány. Uživatelé proto musí mít přístup k informacím o tom, jak doporučující systém vybírá zobrazované informace, případně jim musí být umožněno ovlivnit způsob, jakým jsou jim informace předkládány.

a) Co je to doporučovací systém?

Typickými příklady doporučovacího systému jsou např. newsfeedy, personalizovaná doporučení, našeptávače, způsob řazení nabídky produktů na online tržišti nebo řazení odpovědí ve vyhledávání. Nespadají sem naopak kurátorská a redakční doporučení, neboť nejsou založena na automatizovaném systému.

b) Jaké mají poskytovatelé ve vztahu k uživatelům povinnosti?

Poskytovatel má povinnost uvést hlavní parametry, které jeho doporučovací systém používá, ve svých smluvních podmínkách, kde musí dále uvést, zda může uživatel tyto hlavní parametry měnit či ovlivňovat. Příklady hlavních parametrů mohou být cena, datum, hodnocení spotřebitelů či počet zobrazení. Poskytovatel nicméně nemá povinnost zveřejňovat podrobné technické parametry fungování svého doporučovacího systému ani algoritmy.

Pokud poskytovatel používá více hlavních parametrů pro určení relativního pořadí prezentovaných informací, musí uživatelům umožnit kdykoliv si vybrat a změnit preferovanou možnost. Tato funkce musí být snadno dostupná přímo v části online rozhraní poskytovatele, kde jsou dané informace prezentovány.

Poskytovatelé velmi velkých online platforem a velmi velkých internetových vyhledávačů mají nad rámec výše uvedeného povinnost **poskytnout uživatelům alespoň jednu možnost zobrazení obsahu, která není založena na profilování**, tj. možnost zcela vypnout doporučovací algoritmy.

6.7. Archiv reklam

Poskytovatelé **velmi velkých online platforem a velmi velkých internetových vyhledávačů** musí na svých internetových stránkách zpřístupnit zpětně minimálně po dobu jednoho roku informace o veškeré reklamě, která byla prezentována v jejich online rozhraní. Veřejnost tak má snadný přístup k informacím o tom, jaké reklamy byly na platformě prezentovány, kdo byl jejich zadavatelem nebo jaká byla kritéria pro cílení reklamy.

7. Pravidla moderace obsahu

Digitální zprostředkovatelské služby umožňují uživatelům v reálném čase sdílet s ostatními uživateli nejrůznější informace, názory, obrázky, videa či jiný obsah. Stejně jako ve skutečném světě však mohou být některé tyto informace v rozporu se zákonem nebo s pravidly stanovenými poskytovatelem služby. Nařízení DSA proto zavádí jednotný rámec pro oznamování nezákonného obsahu ze strany veřejnosti a reguluje, za jakých okolností a jakým způsobem mohou poskytovatelé zasahovat do uživatelského obsahu. Pravidla tak chrání uživatele před nepřiměřenými zásahy poskytovatelů do svobody projevu a současně motivují poskytovatele k boji se skutečně nebezpečným obsahem.

7.1. Oznamování nezákonného obsahu

Uživatelé hostingových služeb mohou pomocí elektronických prostředků **oznamovat poskytovateli výskyt konkrétních informací v rámci používané služby, které uživatel považuje za nezákonný obsah.**

a) Co se rozumí nezákonným obsahem?

Nezákonný obsah jsou jakékoli informace včetně zboží a služeb, které nejsou v souladu s právem EU nebo právem některého členského státu, které je v souladu s právem Unie. Nařízení DSA tedy nestanovuje, co je nezákonné, to musí vždy určit zvláštní předpis. Smyslem je, aby jednání, které je nelegální offline, bylo nelegální i online. Jedná se např. o porušování autorského práva, nenávistné projevy, teroristický obsah, prodej zakázaných nebo padělaných výrobků, dětskou pornografii, navazování kontaktu s dětmi za sexuálním účelem, nelegální prodej zvířat, internetové podvody nebo šíření škodlivého softwaru. Legalitu obsahu posuzují v první řadě sami poskytovatelé dle národního práva a nepotřebují k tomu předchozí stanovisko orgánu veřejné moci.

b) Jaké má mít oznámení nezákonného obsahu náležitosti?

Oznámení nezákonného obsahu podané uživateli by mělo podle nařízení DSA obsahovat náležitosti uvedené níže. Poskytovatel musí zajistit, aby bylo podání oznámení pro uživatele **jednoduché a co nejvíce uživatelsky vstřícné** a aby oznámení podávané uživateli obsahovalo alespoň tyto prvky:

- a. **Dostatečně podložené vysvětlení důvodů**, proč se oznamovatel domnívá, že předmětné informace představují nezákonný obsah,
- b. **Vymezení přesného elektronického umístění těchto informací**, ideálně ve formě URL adresy, případně popis umožňující přesně a jednoznačně nalézt a identifikovat nezákonný obsah,
- c. **Jméno nebo název oznamovatele** a jeho **e-mailovou adresu**⁴.
- d. Prohlášení oznamovatele potvrzující, že se v dobré víře domnívá, že informace obsažené v oznámení jsou přesné a úplné.

Poskytovatel naopak po oznamovateli nemůže povinně vyžadovat přesnou právní kvalifikaci protiprávního jednání. Je také důležité zmínit, že podle nařízení DSA musí poskytovatel umožnit oznamování pouze nezákonného obsahu. Pro nahlašování porušení smluvních podmínek režim podle nařízení DSA neplatí.

1. Postup po obdržení oznámení přes mechanismus **Potvrzení oznámení**. Pokud oznamovatel uvedl svůj e-mail, poskytovatel mu na něj bezodkladně zašle **potvrzení o obdržení oznámení**.
2. **Rozhodnutí o oznámení a přijetí opatření**. Poskytovatel poté bez zbytečného odkladu rozhodne, zda považuje dotčený obsah nezákonný či nikoli. **O svém rozhodnutí musí poskytovatel obratem informovat oznamovatele** včetně toho, zda při rozhodování využil automatizované nástroje. Podoba případného opatření je věcí poskytovatele, musí však být přiměřená situaci. Může jít např. o odstranění obsahu nebo jeho znepřístupnění. Individuální méně závažný incident by neměl být důvodem ke smazání nebo pozastavení celého uživatelského účtu.
3. **Poučení o možnostech nápravy. Spolu s rozhodnutím poskytovatel oznamovali zašle i poučení o dostupných možnostech obrany.** Těmi může být využití interního systému vyřizování stížností (pokud jej má poskytovatel zřízen), předložení věci k posouzení subjektu mimosoudního řešení sporů nebo soudní přezkum.

ČTÚ poznamenává, že **poskytovatel nemá podle čl. 16 nařízení DSA povinnost přijmout opatření proti nezákonnému obsahu, o kterém se dozví**. Nicméně pokud poskytovatel nebude konat, má se za to, že na základě oznámení získal dostatečnou povědomost o daném nezákonném obsahu, bude za něj spoluodpovědným a dotčené osoby jej mohou žalovat u soudu dle vnitrostátního práva nebo může být

⁴ V některých případech identifikace není nutná, zejména pokud jsou předmětem oznámení trestné činy uvedené v čl. 3 až 7 směrnice 2011/93/EU (pohlavní zneužívání dětí, dětská pornografie, navazování kontaktu s dětmi k sexuálním účelům).

trestně či správně odpovědným. **Úkolem ČTÚ jako dozorového orgánu není posuzovat, zda oznámený obsah byl nebo nebyl nezákonný**, ale pouze dohlédnout na to, zda poskytovatel v procesu vyřizování oznámení dodržel všechny povinnosti podle nařízení DSA.

Příklad 3: Uživatel registrovaný na sociální síti XY je známý hudebník. Během své 14denní dovolené v Egyptě zjistí, že se na této sociální síti začalo masově šířit video, jehož součástí je i jedna z jeho skladeb, ačkoli k tomu nedal souhlas. Rozhodne se proto obsah oznámit poskytovateli jako nezákonný. Po přihlášení do online rozhraní však zjistí, že funkce pro oznámení nezákonného obsahu není dostupná. Zákaznická podpora poskytovatele mu později sdělí, že tato funkce je dostupná pouze na území EU.

Vysvětlení: Poskytovatel porušil nařízení DSA, neboť uživateli omezil jeho práva pouze na základě skutečnosti, že se dočasně nacházel mimo území EU, ačkoli si vzhledem k jeho uživatelské historii musel být vědom, že je občanem EU.

Příklad 4: Uživatel zaslal poskytovateli hostingové služby oznámení o nezákonném obsahu v podobě sdílení nelegální kopie hudební nahrávky. Poskytovatel oznámený obsah obratem odstranil, avšak nezaslal uživateli ani potvrzení o přijetí oznámení, ani rozhodnutí, jak oznámení posoudil. Na pozdější dotaz uživatele svůj postup odůvodnil tím, že oznámený obsah byl kromě zákona v rozporu i se smluvními podmínkami poskytovatele, proto poskytovatel věc kvalifikoval jako porušení smluvních podmínek a nepostupoval podle čl. 16 nařízení DSA.

Vysvětlení: Poskytovatel porušil nařízení DSA, neboť měl podnět vyřídit jako oznámení nezákonného obsahu. Poskytovatel nemůže svévolně rozhodnout o tom, že oznámení nelegálního obsahu překvalifikuje na porušení smluvních podmínek.

7.2. Odůvodnění omezení

a) Kdy musí poskytovatel poskytnout uživateli odůvodnění?

V případě jakéhokoli omezení uživatelského obsahu ze strany poskytovatele hostingové služby musí takto postižený uživatel od poskytovatele obdržet jasné a konkrétní odůvodnění, a to bez ohledu na to, zda byla důvodem omezení nezákonnost obsahu nebo neslučitelnost se smluvními podmínkami. Uvedené se týká např. smazání příspěvku na sociální síti, označení e-mailu za spam nebo odstranění uživatelského účtu.

b) Co musí odůvodnění obsahovat?

Odůvodnění poskytnuté poskytovatelem musí být jasné, snadno srozumitelné a co nejpřesnější a nejkonkrétnější s ohledem na okolnosti případu, tak aby byl dotčený uživatel schopen pochopit důvody uloženého omezení, proto musí obsahovat minimálně tyto informace:

- **v čem spočívá uložené omezení**, např. odstranění informací, znemožnění přístupu k nim, přiřazení horší pozice ve vyhledávání, omezení jejich viditelnosti nebo pozastavení či ukončení peněžních plateb souvisejících s těmito informacemi, **jaké jsou jeho důsledky**, případně jeho územní působnost a dobu platnosti,
- **skutečnosti a okolnosti, na základě kterých bylo rozhodnutí přijato**,
- v relevantních případech informace o použití automatizovaných postupů při přijímání rozhodnutí,
- v případě nezákonného obsahu odkaz na příslušný právní předpis a vysvětlení, proč se informace z tohoto důvodu pokládají za nezákonný obsah,

- v případě porušení smluvních podmínek odkaz na příslušné ustanovení smluvních podmínek a vysvětlení, proč se informace pokládají za neslučitelné s příslušným ustanovením,
- **informace o možnostech obrany**, které má příjemce služby k dispozici, zejména prostřednictvím interního systému vyřizování stížností (je-li k dispozici), mimosoudního řešení sporů a soudního přezkumu.

c) Kdy musí uživatel obdržet odůvodnění?

Uživatel musí odůvodnění obdržet nejpozději v den, kdy mu bylo omezení uloženo. Z uvedeného pravidla nařízení DSA připouští tři výjimky. Uživatel nemusí obdržet odůvodnění pokud:

- a) poskytovateli nejsou známy elektronické kontaktní údaje uživatele;
- b) uživatel úmyslně zneužil služby k šíření klamavého obchodního obsahu ve velkém objemu, např. pomocí botů či falešných účtů,
- c) poskytovatel postupuje podle čl. 9 nařízení DSA.

d) Další povinnosti poskytovatelů vůči uživatelům

Podobně musí uživatel obdržet písemné odůvodnění, včetně uvedení dostupných možností nápravy a popisu územní působnosti, pokud poskytovatel na základě příkazu justičního nebo správního orgánu přijal opatření proti nezákonnému obsahu poskytovaného uživatelem nebo v případě žádosti o poskytnutí určitých informací o uživateli. Orgán vydávající příkaz však může v zájmu utajení trestního řízení rozhodnout, že se odůvodnění neposkytne nebo poskytne později.

Pokud vyjde najevo, že uživatel online platformy **často poskytuje zjevně nezákonný obsah**, poskytovatel jej na toto jednání **upozorní**, a pokud v této činnosti i přesto pokračuje, **pozastaví uživateli poskytování služeb**. Obdobně poskytovatel pozastaví vyřizování oznámení podle čl. 16 a stížností podle čl. 20 nařízení DSA osobám, které často podávají zjevně neodůvodněná oznámení a stížnosti. Za zjevné zneužití se považují ty případy, kdy je i neoborníkovi zřejmé, že obsah je nezákonný nebo že jsou oznámení nebo stížnosti nepodložené. Dotčený uživatel musí od poskytovatele obdržet odůvodnění takového postupu včetně poučení o možnostech obrany.

V neposlední řadě je třeba zmínit, že nařízení DSA dopadá jen na moderaci prováděnou poskytovatelem služeb, pokud opatření provedl např. autor blogu nebo správce komunity, nařízení DSA se nepoužije.

Příklad 5: Poskytovatel online platformy rozhodl o smazání videa uživatele, neboť jeho interní systém detekoval, že jde o neoprávněné užití autorského díla. Dotčenému uživateli následně byla následující den zaslána notifikace, kterou byl krátce informován, že došlo k odstranění jím nahraného obsahu z důvodu porušení zásad komunity.

Vysvětlení: Poskytovatel porušil nařízení DSA, neboť odůvodnění svého opatření, které zaslal uživateli, nebylo dostatečně konkrétní ani odůvodněné a neobsahovalo poučení o možnostech nápravy. Odůvodnění musí obsahovat popis jednání, které bylo důvodem pro rozhodnutí o omezení a odkaz na konkrétní ustanovení smluvních podmínek, případně právního předpisu, na základě kterých bylo toto rozhodnutí přijato. Poskytovatel rovněž pochybil, když uživatele o svém opatření neinformoval ještě tentýž den.

Příklad 6: Uživatel AB zveřejnil na sociální síti příspěvek, pod kterým následně začali zveřejňovat své komentáře ostatní uživatelé. Uživatel XY ve svých komentářích označil uživatele AB za lháře a nelichotivě se zmínil o jeho vzhledu. O několik hodin později si uživatel XY všiml, že jeho komentáře pod příspěvkem zmizely. Zaslal proto stížnost poskytovateli, ve které se dožadoval patřičného

zdůvodnění. Poskytovatel odpověděl, že předmětnou moderaci obsahu provedl pomocí příslušné funkce uživatel AB a tudíž za ni neodpovídá.

Vysvětlení: Poskytovatel se nedopustil porušení nařízení DSA, když nezaslal uživateli odůvodnění smazání komentářů, neboť podle nařízení DSA musí odůvodnit jen svá vlastní moderační opatření.

7.3. Interní systém vyřizování stížností

Uživatelé online platform (mimo malé a mikro podniky) včetně oznamovatelů podle čl. 16 nařízení DSA mají právo napadnout rozhodnutí poskytovatele podáním interní stížnosti. Napadnout lze rozhodnutí týkající se nezákonnosti obsahu i jeho neslučitelnosti se smluvními podmínkami.

a) Jaké typy stížností mohou uživatelé přes interní systém podávat?

Stížnost musí být možné podat elektronicky, bezplatně a uživatelsky přívětivým způsobem, např. formou snadno přístupného online formuláře na internetových stránkách poskytovatele. Napadnout lze minimálně tato rozhodnutí poskytovatele:

- rozhodnutí o (ne)odstranění informace, (ne)znemožnění přístupu k ní nebo (ne)omezení její viditelnosti,
- rozhodnutí o úplném nebo částečném pozastavení či ukončení poskytování služby příjemci,
- rozhodnutí o pozastavení či ukončení uživatelských účtů příjemců,
- rozhodnutí o pozastavení, ukončení nebo jiném omezení monetizace informací poskytnutých příjemcem.

b) Jaký je postup při podávání stížností přes interní systém?

Stížnost je možné podat nejpozději do 6 měsíců ode dne, kdy byl uživatel informován o rozhodnutí poskytovatele. Uživatel má rovněž **právo, aby se na rozhodování podílel lidský prvek**, rozhodnutí proto nesmí být vydáno pouze na základě automatizovaných nástrojů.

O výsledku stížnosti poskytovatel bez zbytečného odkladu informuje stěžovatele včetně odůvodnění svého závěru a poučení o možnostech obrany v podobě mimosoudního řešení sporů nebo soudního přezkumu. Pokud poskytovatel na základě stížnosti dospěje k závěru, že napadené rozhodnutí bylo nesprávné, předmětné rozhodnutí bez zbytečného odkladu zruší, tj. např. obnoví poskytování služeb v původním rozsahu.

7.4. Systém mimosoudního řešení sporů

Uživatelé a oznamovatelé se mohou proti rozhodnutím poskytovatele online platformy (s výjimkou malých a mikro podniků) bránit u subjektu mimosoudního řešení sporů. Uživatel si může vybrat kterýkoli subjekt usazený v EU certifikovaný příslušným koordinátorem digitálních služeb, který má odbornost pro danou oblast sporů.

a) Kdy se mohou uživatelé bránit u subjektu mimosoudního řešení sporů?

Podmínkou zahájení tohoto řízení není předchozí využití interního systému vyřizování stížností. Naopak není možné takto napadnout případy, o kterých už bylo jednou rozhodnuto nebo jsou předmětem probíhajícího řízení. Totožnost věci je dána zejména pokud se jedná o stejné dotčení

informace, důvody pro přijetí napadeného rozhodnutí, účinky rozhodnutí a důvody pro napadení rozhodnutí. **Rozhodnutí by mělo být vydáno do 90 dnů**, ve složitějších případech do 180 dnů. **Subjekt mimosoudního řešení sporů nemá pravomoc uložit stranám závazné řešení sporu** a věc je možné kdykoli předložit k posouzení soudu.

b) Náklady řízení

Podání návrhu je pro uživatele bezplatné nebo za nominální poplatek. Výši poplatku je subjekt mimosoudního řešení sporů povinen uživateli sdělit před zahájením řízení. V případě úspěchu uživatele má poskytovatel povinnost uhradit mu veškeré poplatky účtované subjektem mimosoudního řešení sporů a dále mu nahradit všechny přiměřené výdaje, které v souvislosti s řešením sporu zaplatil. Přiměřenost výdajů je dle názoru ČTÚ nutné vztahovat k jejich objektivní účelnosti. V případě neúspěchu uživatele nemá poskytovatel nárok na náhradu žádných nákladů, ledaže prokáže, že uživatel jednal ve zlém úmyslu.

8. Ochrana uživatelů online platformem

V oblasti bezpečnosti a ochrany uživatelů nařízení DSA reaguje na trend rostoucí popularity online platformem a stanovuje pro ochranu uživatelů podobná pravidla, jakými byly doposud chránění pouze spotřebitelé. Vedle toho je kladen velký důraz na zvýšenou ochranu dětí v online prostoru, které mohou být obzvláště zranitelné vůči různým nelegálním praktikám. V neposlední řadě nařízení DSA stanovuje pravidla pro prezentaci online reklamy.

8.1. Zákaz dark patterns

Poskytovatelé nesmí v rámci svých online rozhraní (tj. jakýkoliv software – internetové stránky či aplikace) zavádět tzv. dark patterns.

a) Co jsou tzv. dark patterns?

Dark patterns (česky temné vzorce) jsou praktiky, které klamou, manipulují či jinak podstatně narušují nebo omezují schopnost uživatelů činit svobodná a informovaná rozhodnutí. Může se jednat o soubor řešení uživatelského rozhraní, která jsou navržena tak, aby uživatele záměrně přiměla k akci, která je žádoucí z pohledu poskytovatele, ale pro uživatele má negativní důsledky.

b) Příklady dark patterns

Nařízení DSA zakazuje poskytovatelům online platformem (s výjimkou malých a mikro podniků) používání jakýchkoli praktik dark patterns. **Poskytovatelé nesmějí své online rozhraní koncipovat, uspořádat ani provozovat způsobem, který klame uživatele jejich služby nebo jimi manipuluje, či jinak podstatně narušuje či omezuje schopnost uživatelů jejich služeb činit svobodná a informovaná rozhodnutí.**

Nařízení DSA chrání uživatele mimo jiné proti těmto praktikám:

- přednostní zvýrazňování určitých možností volby v situaci, kdy je po příjemci služby požadováno, aby učinil rozhodnutí,
- opakované žádosti, aby příjemce služby provedl výběr v okamžiku, kdy tento výběr již byl proveden, zejména otevíráním nabídkových oken apod.,
- ztěžování ukončení služby nebo zrušení předplatného ve srovnání s aktivací služby nebo ztěžování vyjádření nesouhlasu,

- skryté či přednastavené souhlasy nebo nefunkční možnosti volby,
- zavádějící nabídky,
- skryté poplatky,
- přidávání zboží do košíku bez souhlasu příjemce služby,
- vytváření nátlaku pomocí časově velmi omezených nabídek nebo vyvolávání dojmu, že nabídka bude brzy nedostupná,
- emocionální nátlak,
- falešné recenze.

c) Co naopak nejsou dark patterns podle nařízení DSA?

Úprava podle nařízení DSA se naopak nepoužije na situace, které už jsou regulovány nařízením GDPR nebo předpisy na ochranu spotřebitele. Do působnosti nařízení DSA tak nebude spadat např. manipulativní cookies lišta nebo agresivní obchodní praktiky vůči spotřebiteli. Největší přínos tohoto ustanovení lze proto čekat zejména ve vztahu k nespotřebitelům a v situacích, kdy uživatel nejedná v souvislosti s nákupem zboží nebo služeb.

Bližší informace o tom, co jsou dark patterns jsou k dispozici také na webových stránkách Evropské Komise [Akt o digitálních službách: Otázky a odpovědi](#).

8.2. Ochrana nezletilých osob

Děti či nezletilí, kteří jsou dnes často označováni jako tzv. digitální generace, běžně využívají digitální služby k nejrůznějším činnostem. Zároveň jsou děti považovány za zvláště zranitelné osoby, které by měly být v digitálním prostředí chráněny, protože si mohou být s ohledem na svůj věk a rozumovou vyspělost méně vědomy rizik, důsledků a záruk svých práv v souvislosti se zpracováním informací, které zobrazují v digitálním prostředí. Zvláštní ochrana dětí by se měla např. vztahovat na používání jejich osobních údajů pro účely marketingu, vytváření osobnostních či uživatelských profilů a využívání služeb nabízených přímo dětem.

V souvislosti s ochranou dětí se obecně uplatní institut nejlepšího zájmu dítěte, který je zakotven v mezinárodních předpisech a promítá se i do evropského a vnitrostátního práva. Dosud byla v online oblasti poskytována nezletilým ochrana především prostřednictvím právního rámce ochrany osobních údajů a uplatnění jeho zásad, nicméně nařízení DSA, které považuje ochranu dětí za jednu ze svých priorit, ji rozšiřuje ve vztahu k digitálním službám jako k celku, takže přináší více možností ochrany práv dětí. Dále chrání nezletilé uživatele před jakýmkoli manipulativními praktikami, které by využívaly jejich zranitelnosti a nezkušenosti.

a) Jaká opatření na ochranu nezletilých jsou povinni poskytovatelé zavést?

Poskytovatelé online platform (s výjimkou malých a mikro podniků) přístupných nezletilým osobám jsou proto povinni zavést vhodná a přiměřená opatření, kterými **zajistí vysokou míru soukromí, bezpečnosti a ochrany nezletilých osob v rámci svých služeb.**

Příkladem možných opatření k zajištění souladu služby s nařízením DSA jsou:

- systémy ověřování věku uživatelů u služeb, které obsahují pro nezletilé nevhodný nebo zakázaný obsah,
- nastavení výchozího online rozhraní nezletilých osob na nejvyšší úroveň ochrany soukromí,
- minimalizace sběru dat,

- zákaz sdílení polohy,
- nepoužívání praktik, které mohou u nezletilých způsobovat závislost,
- přijetí opatření proti navazování kontaktu s nezletilými za sexuálními účely,
- zavedení systémů rodičovské kontroly,
- účinná věková omezení dostupnosti určitých služeb,
- aktivní monitorování a moderace nezákonného obsahu nebo
- vytváření bezpečných zón určených pouze pro nezletilé.

Důležitým obecným pravidlem ve vztahu k nezletilým je, aby jim byly veškeré informace a sdělení podávány za použití jasných a jednoduchých jazykových prostředků, aby jim děti snadno porozuměly.

Dalším opatřením v nařízení DSA je **zákaz profilování** zakotvený v článku 28 odst. 2, který je popsán níže v části **Chyba! Nenalezen zdroj odkazů.** - Regulace online reklamy.

8.3. Regulace online reklamy

Reklama je v online prostředí významným fenoménem a pravidelně tvoří významný podíl informací zobrazovaných na online platformách příjemcům služeb. Příjemce služeb je často v situaci, kdy neví, za jakých podmínek se reklama zobrazuje a zda a jak ji může odmítnout. Reklama přitom může patřit k významným rizikům pro společnost i občany. Ačkoli právní rámec ochrany osobních údajů stanoví požadavky týkající se zpracování osobních údajů, které dopadají i na reklamu na online platformách, které se týkají např. požadavků na cookies či profilování, používání reklamy v online prostředí stále není dostatečně transparentní, a je spojeno se značnými riziky, na což reaguje nařízení DSA.

Reklamou se podle nařízení DSA rozumí informace určené k propagaci sdělení určité právnické nebo fyzické osoby bez ohledu na to, zda má komerční, nebo nekomerční účel, prezentované online platformou na jejím online rozhraní za odměnu výslovně za účelem propagace těchto informací.

Za rizika používání reklamy na online platformách je považováno např. zobrazování nezákonného či závadného obsahu, šíření dezinformací či zacílení na zranitelné společenské skupiny prostřednictvím profilování apod. Tato rizika jsou obzvláště závažná ve vztahu k dětem s ohledem na jejich větší zranitelnost.

a) Jaké mají poskytovatelé povinnosti ve vztahu k online reklamě?

Nařízení DSA na tuto situaci reaguje prostřednictvím požadavků na **transparentnost** reklamy prezentované na online platformách. **Konkrétně toto ukládá poskytovatelům online platform (s výjimkou malých a mikro podniků), kteří na svých online rozhraních prezentují reklamu, povinnost zajistit, aby příjemci služby mohli u každé konkrétní reklamy jasně, stručně a jednoznačně a v reálném čase určit:**

- skutečnost, že informace jsou reklamou,
- osobu, jejímž jménem je reklama prezentována, případně osobu, která reklamu zaplatila,
- smysluplné informace přímo a snadno dostupné z reklamy, jak byl určen jako adresát reklamy, případně jak lze tyto parametry změnit.

Poskytováním informací v souvislosti s reklamou není dotčeno uplatňování příslušných ustanovení nařízení GDPR, zejména ustanovení o právu vznést námitku, o automatizovaném individuálním rozhodování, včetně profilování, a zvláště o potřebě získat před zpracováním osobních údajů pro cílenou reklamu souhlas subjektu údajů.

S ohledem na to, že sami příjemci služeb se mohou podílet na obsahu online platform, zakládá nařízení DSA poskytovatelům online platform povinnost poskytnout příjemcům služby funkci, která příjemcům též umožňuje oznámit, zda obsah, který poskytují, představuje nebo obsahuje obchodní sdělení. V takovém případě poskytovatel zajistí, aby ostatní příjemci služby mohli jasně, jednoznačně a v reálném čase určit, a to i prostřednictvím viditelných označení, že obsah poskytnutý příjemcem služby představuje obchodní sdělení.

Příklad 7: Fyzická osoba (příjemce služeb) se věnuje ve svých příspěvcích na sociální síti módním trendům a recenzím módních doplňků. Zároveň tato osoba sama vyrábí módní doplňky, které v některých svých příspěvcích na sociální síti propaguje. Poskytovatel online platformy (v rámci tohoto příkladu sociální sítě) umožňuje všem osobám, které přispívají svým obsahem na tuto platformu, označit jakýkoliv svůj příspěvek jako představující či obsahující obchodní sdělení. Uvedená fyzická osoba tuto funkcionalitu využije, svůj příspěvek takto označí, a ostatní příjemci služby jasně a v reálném čase mohou seznat, že určité příspěvky jsou obchodním sdělením, které se týkají módních doplňků, jež osoba vyrábí.

b) Zákaz profilování

Nařízení DSA zároveň stanovuje pro poskytovatele dva zákazy, které se týkají profilování⁵ za použití osobních údajů. Předně je **zakázáno**, aby poskytovatel online platformy prezentoval příjemcům služby reklamy na základě profilování ve smyslu nařízení GDPR, které využívá zvláštní kategorie osobních údajů podle čl. 9 odst. 1 nařízení GDPR, např. údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání, o zdravotním stavu, sexuální orientaci osoby apod.

Příklad 8 – profilování osobních údajů zvláštní kategorie: Společnost odvozuje náboženské přesvědčení osob z obsahu příspěvků (např. příspěvky o návštěvě bohoslužebných míst) a poté na základě těchto informací zobrazuje reklamu.

Pokud jde o ochranu nezletilých na internetu, čl. 28 odst. 2 nařízení DSA striktně **zakazuje**, aby poskytovatelé online platform na svém rozhraní prezentovali reklamy založené na profilování ve smyslu nařízení GDPR za použití osobních údajů příjemce služby, pokud jsou si poskytovatelé služeb s přiměřenou jistotou vědomi toho, že příjemcem služby je nezletilá osoba.

8.4. Ochrana spotřebitelů na online tržištích

Online platformy umožňující spotřebitelům uzavírat s obchodníky smlouvy na dálku neboli online tržiště, tvoří důležitou součást digitální ekonomiky, neboť zprostředkovávají čím dál větší podíl obchodní výměny mezi podnikateli a spotřebiteli. Nařízení DSA proto usiluje o to, aby zde platily podobné standardy ochrany spotřebitele, které platí v případě přímého prodeje v e-shopech.

a) Jaké informace o obchodnících a produktech musí poskytovatel zveřejnit?

Informace o obchodnících:

Na online tržištích (s výjimkou malých a mikro podniků) nemohou své zboží a služby nabízet obchodníci, o kterých poskytovatel nezískal dostatečné informace. Přímo v online rozhraní, kde jsou

⁵ **Profilováním** se podle nařízení GDPR rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu. Profilování může být užito za účelem ovlivnění přijetí rozhodnutí určitého subjektu, a proto je podrobeno podrobnější regulaci nejen v rámci nařízení DSA, ale i v rámci nařízení GDPR.

prezentovány nabídky zboží či služby, pak musí být pro uživatele dostupné v jasné, snadno přístupné a srozumitelné formě tyto údaje o obchodnících:

- a) Jméno, poštovní adresa, telefonní číslo a emailová adresa obchodníka;
- b) Identifikační číslo v případě, pokud je obchodník zapsán v některém z relevantních rejstříků;
- c) Autocertifikace obchodníka, kterou se zavazuje prodávat pouze ty produkty, které jsou v souladu s národním, či evropským právem.

Zveřejnění těchto údajů má především za cíl odradit nepoctivé obchodníky a posílit pozici spotřebitele v případě, že bude chtít obchodníka kontaktovat např. z důvodu reklamace nebo odstoupení od smlouvy.

b) Informace o zboží a službách

Obchodníci by měli mít prostor zveřejnit u svých produktů zákonem předepsané předsmulovní informace, informace o bezpečnosti výrobků a informace nezbytné pro jasnou a jednoznačnou identifikaci nabízeného zboží nebo služeb, identifikující znak obchodníka (ochrannou známku, symbol, logo etc.) a dále informace o případných označeních či jiných značkách dle právních předpisů v oblasti bezpečnosti výrobků.

c) Ověřování nezákonných produktů

Nařízení DSA také zvyšuje bezpečnost nabízeného sortimentu, neboť poskytovatel online tržiště má povinnost průběžně **namátkově ověřovat, zda nebyly výrobky nebo služby nabízené obchodníky označeny za nezákonné.**

Pokud spotřebitel zakoupí nezákonné zboží nebo službu a poskytovatel online tržiště se o tom dozví nejpozději do 6 měsíců od dokončení nákupu, je povinen o tom spotřebitele informovat včetně totožnosti obchodníka a poučení o relevantních možnostech nápravy. Jestliže poskytovatel nedisponuje kontaktními údaji všech dotčených spotřebitelů, zveřejní dané informace alespoň na svém online rozhraní.

8.5. Ochrana před systémovými riziky

Vedle nezákonného obsahu nařízení DSA pomáhá chránit uživatele také před tzv. systémovými riziky, která jsou spojena **vylučně** s fungováním velmi velkých online platforem a velmi velkých internetových vyhledávačů. Jejich poskytovatelé mají povinnost průběžně analyzovat možné negativní dopady svých služeb na jednotlivé uživatele i společnost, neboť jsou to právě velké globální digitální platformy, které zásadním způsobem formují podobu online prostoru a jeho bezpečnost.

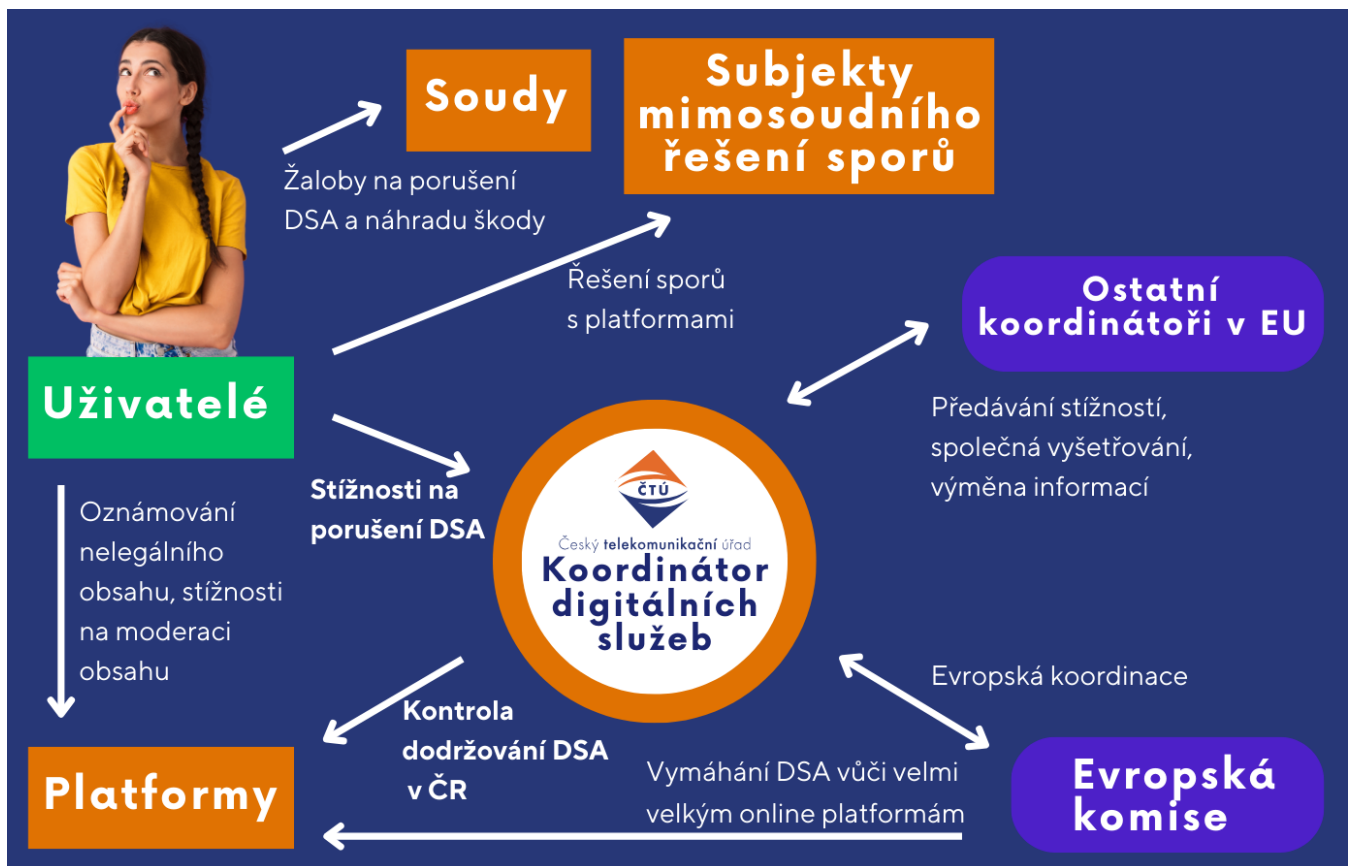
Systémová rizika zahrnují např. šíření nezákonného obsahu, vyvolávání závislosti, nepříznivé dopady na základní lidská práva včetně ochrany svobody projevu, občanský diskurz, volební procesy, veřejnou bezpečnost či ochranu spotřebitele. **Smyslem pravidel je, aby velké online platformy negativní společenské jevy v online prostoru nepříživovaly např. za účelem zvýšení dosahu příspěvků či monetizace, nýbrž utlumovaly.**

Opatření proti systémovým rizikům nemusí mít nutně podobu odstraňování problematických příspěvků nebo uživatelských účtů, může se jednat o přiměřenou úpravu online rozhraní či smluvních podmínek, změnu nastavení doporučovacíh algoritmů, prevenci zakládání falešných uživatelských účtů, označování problematického obsahu, umožnění uživatelům zvolit si, který obsah nechtějí, aby jim byl prezentován, nebo zajištění dostatečné personální kapacity pro moderaci obsahu. Dostatečnost těchto

opatření posuzuje Evropská komise, uživatelé však mohou dozorové orgány formou stížnosti upozornit na případná nedostatečná opatření ze strany platformem.

9. Dozor nad dodržováním povinností

Podle čl. 49 odst. 1 nařízení DSA musí každý členský stát Evropské unie určit tzv. „koordinátora digitálních služeb.“ **V České republice byl koordinátorem určen ČTÚ.** Koordinátor digitálních služeb odpovídá za veškeré záležitosti související s vnitrostátním dozorem podle nařízení DSA, pokud nebyly svěřeny jinému orgánu. Jeho povinností je vykonávat svěřené úkoly nestranně, nezávisle, transparentně a včas. Dozor nad čl. 26 a 28 odst. 2 nařízení DSA týkající se online reklamy vykonává **Úřad pro ochranu osobních údajů.** Porušení povinností stanovených nařízením DSA je přestupkem, za který hrozí poskytovatelům **pokuta až do výše 6 % celosvětového ročního obrátu.**



10. Jak podat stížnost

h) Jak mohou uživatelé podat stížnost?

Kterýkoli **uživatel má právo má právo podat stížnost koordinátorovi digitálních služeb**, pokud se domnívá, že dochází k porušování nařízení DSA. Podnět je možné ČTÚ podat osobně, poštou nebo elektronicky do e-mailové schránky podatelna@ctu.cz, do datové schránky ID: a9qaats nebo prostřednictvím [online formuláře](#). ČTÚ upozorňuje, že aby mohla být stížnost vyřízena, musí se týkat porušení některé z povinností podle nařízení DSA. **Stížnost neslouží k řešení sporů uživatele s poskytovatelem ohledně charakteru (ne)smazaného obsahu ani sporů mezi uživateli navzájem.**

i) Co může být předmětem stížnosti?

Před podání stížnosti ČTÚ doporučuje vyčerpat všechny možnosti nápravy, které poskytovatel nabízí, tj. např. kontaktovat poskytovatele, oznámit nezákonný obsah nebo využít interní systém vyřizování stížností.

Předmětem stížnosti může být jakákoli povinnost poskytovatele, resp. právo uživatele podle nařízení DSA, například:

- nefunkční kontaktní místo,
- uplatňování nepřiměřených omezení služeb,
- nemožnost odeslat poskytovateli oznámení o nezákonném obsahu,
- neposkytnutí odpovědi na oznámení nezákonného obsahu,
- neposkytnutí odůvodnění při odstranění uživatelského účtu nebo konkrétního obsahu,
- neoprávněné odstranění uživatelského účtu nebo konkrétního obsahu,
- klamavé nebo manipulativní praktiky poskytovatele,
- neuvedení informací o online reklamě,
- neuvedení hlavních parametrů řazení zobrazeného obsahu,
- nezajištění dostatečné ochrany nezletilých uživatelů,
- neuvedení dostatečných informací o obchodnících na online tržišti.

j) Jaký je postup ČTÚ po podání stížnosti?

ČTÚ stížnost posoudí do 30 dnů a v případě zjištění pochybení poskytovatele zahájí kontrolu nebo řízení o přestupku. Pokud vyjde najevo, že stížnost spadá do působnosti jiného úřadu, ČTÚ mu stížnost postoupí. V případě, že ČTÚ vyhodnotí, že stížnost by mohla být důvodná, ale směřuje proti poskytovateli, který sídlí v jiném členském státě EU, může ji spolu se svým stanoviskem postoupit koordinátorovi digitálních služeb tohoto členského státu. Poté, co je stížnost postoupena, je za její vyřízení a posouzení odpovědný zahraniční koordinátor. ČTÚ nemůže nijak ovlivnit, jak zahraniční koordinátor se stížností naloží.

V zájmu objektivního prošetření věci ČTÚ doporučuje stěžovatelům, aby u každé stížnosti podrobně popsali, které služby a kterého poskytovatele se stížnost týká a dále uvedli, v čem konkrétně spatřují porušení nařízení DSA. Stížnost by rovněž měla být podložena co největším množstvím důkazů jako např. URL adresa, printscreeny obrazovky či kopie veškeré komunikace s poskytovatelem.

11. Právo uživatelů na náhradu škody

Většina povinností pro poskytovatele služeb podle nařízení DSA zakládá současně právo pro uživatele, jehož se lze domáhat soudní cestou zcela nezávisle na výkonu dozorové působnosti ze strany ČTÚ. **Jestliže uživateli vznikla škoda nebo ztráta v důsledku porušení povinností poskytovatele podle nařízení DSA, má právo po poskytovateli požadovat náhradu.** O přiznání náhrady škody rozhodují obecné soudy nikoli ČTÚ. Spotřebitelé mohou kteréhokoli poskytovatele usazeného v EU žalovat u soudu dle místa svého bydliště, ostatní uživatelé musí provozovatele žalovat v zemi jeho usazení.

Podle čl. 90 nařízení DSA mohou žaloby na porušení tohoto nařízení, která poškozují nebo mohou poškodit kolektivní zájmy spotřebitelů, podávat také organizace chránící spotřebitele.

12. Další zdroje

Podrobnější informace o právech uživatelů podle nařízení DSA lze rovněž nalézt v následujících materiálech uveřejněných Evropskou Komisí nebo Ministerstvem průmyslu a obchodu (MPO):

- **Zdroje Evropské Komise:**
 - [Akt o digitálních službách: Otázky a odpovědi](#)
 - [Nařízení o digitálních službách \(DSA\) vysvětlení – Opatření na ochranu dětí a mládeže na internetu](#)
- **Zdroje MPO:**
 - [Nařízení o digitálních službách](#)
 - [Co znamená DSA pro uživatele?](#)
 - [Q&A k moderování obsahu podle DSA \(brožura\)](#)

Příloha: Vzor stížnosti

Stížnost

Jméno a příjmení stěžovatele např.: Jan Novák

Kontaktní údaje stěžovatele např.: novak.jan@email.cz

Vážená paní/Vážený pane,

tímto podávám stížnost na poskytovatele služeb XY s.r.o., jehož služby jsou poskytovány prostřednictvím internetové stránky XY.cz.

... (vyličení všech důležitých skutečností, tj. co, kdy, kde a jak se stalo, ideálně s označením důkazů) ...

např. poskytovatel neumožňuje uživatelům nahlásit obsah, který může být považován za nezákonný. Na této platformě jsem dne 31. 10. 2024 narazil na příspěvky, které obsahují nezákonný obsah. U těchto příspěvků ani nikde jinde na webu jsem však nenašel nástroje k jejich nahlášení. Dle čl. 15 DSA by takový mechanismus měl být jednoduše přístupný.

Žádám proto o prošetření věci.

Příloha:

Printscreen internetové stránky

URL adresa dotčeného obsahu

Kopie komunikace s poskytovatelem