

Bird & Bird &

Aktuality z EÚ legislatívy

Júl 2021

V tomto letnom vydaní Aktualít z EÚ legislatívy Vám prinášame prehľad z európskej legislatívy za nedávne obdobie. Hádám najväčšou a dlhou očakávanou novinkou je **návrh nariadenia o umelej inteligencii**. Nariadenie je postavené na prístupe založenom na hodnotení rizika a regulácia jednotlivých systémov umelej inteligencie sa odvíja od kategorizácie systému s ohľadom na riziko. Prinášame Vám tiež zhrnutie zo spoločného stanoviska, ktoré k tomuto návrhu prijali Európsky dozorný úradník pre ochranu údajov a Európsky výbor pre ochranu údajov, v ktorom sa zamerali na preĺnanie návrhu regulácie umelej inteligencie a regulácie ochrany údajov.

Počas pandémie výrazne vrástli nákupy spotrebiteľov v online prostredí, a to otvorilo otázku **revidovania právneho rámca bezpečnosti tovarov**. V tejto súvislosti Komisia predložila návrh nariadenia s cieľom zachovať úlohu bezpečnostnej siete pre spotrebiteľov a prispôsobiť právny rámec výzvam spojeným s novými technológiami a online predajom.

Podľa nových pravidiel navrhovaných Európskou Komisiou vo forme **Aktu o Údajoch (Data Act)**, ktorý by mal byť publikovaný neskôr tento rok, môžu súkromné spoločnosti čeliť povinnosti umožniť prístup k ich údajom. Stručný náhľad na túto problematiku je spracovaný na základe nedávnej publikácie počítačového posúdenia dopadov.

Nadalej monitorujeme vývoj tzv. Digitálneho balíčka a tentokrát prinášame názory BEREC k **Aktu o digitálnych trhoch**.

Na záver pripájame prehľad aktuálne prebiehajúcich **verejných konzultácií**.

Obsah:

- [1 Regulačný rámec pre umelú inteligenciu](#)
- [2 Nariadenie o umelej inteligencii z pohľadu ochrany osobných údajov](#)
- [3 Ochrana spotrebiteľov v online prostredí](#)
- [4 Akt o údajoch \(„Data Act“\)](#)
- [5 Akt o digitálnych trhoch \(„Digital Markets Act“\) – návrhy od BEREC](#)
- [6 Verejné konzultácie](#)

1. Regulačný rámec pre umelú inteligenciu

Vôbec prvý európsky právny rámec pre umelú inteligenciu

V rámci digitálnej regulačnej agendy Európskej komisie bol 21. apríla zverejnený balík pre umelú inteligenciu („UI“) s cieľom stanoviť globálny zlatý štandard pre reguláciu v tomto sektore. Súčasťou balíka je návrh [Nariadenia, ktorým sa ustanovujú harmonizované pravidlá umelej inteligencie \(Akt o umelej inteligencii\)](#) a menia niektoré legislatívne akty únie („Nariadenie“), ďalej [Koordinačný plán pre členské štáty](#) a [Návrh nariadenia o strojových zariadeniach](#).

Podľa návrhu Nariadenia, ktoré bude priamo uplatniteľné v členských štátoch EÚ a bude mať tiež extra-teritoriálny dosah, sa budú na vývojárov, používateľov, ako aj na dovozcov systémov umelej inteligencie vzťahovať významné nové povinnosti. Podľa návrhu budú zakázané najrizikovejšie systémy, o ktorých sa predpokladá, že sú v rozpore so základnými hodnotami EÚ. Návrh taktiež stanovuje odstrašujúce pokuty pre spoločnosti, ktoré by porušovali pravidlá týkajúce sa údajov, a to vo výške až 30 miliónov EUR alebo 6% celosvetového ročného obratu za predchádzajúci finančný rok.

Niektoré zainteresované strany však už navrhované Nariadenie kritizovali za nejasné a nepresné výrazy a za nedostatok mechanizmov nápravy pre občanov, ktorých by systémy UI negatívne ovplyvnili. K návrhu Nariadenia už prijali spoločné stanovisko Európsky dozorný úradník pre ochranu údajov (European Data Protection Supervisor - EDPS) a Európsky výbor pre ochranu údajov (European Data Protection Board - EDPB), v ktorom sa zamerali na aspekty ochrany osobných údajov a strety medzi reguláciu UI a ochranou údajov. Stručné zhrnutie tohto stanoviska nájdete ďalej v [časti 2](#).

Trojročný proces

Návrh Nariadenia je výsledkom trojročného procesu, ktorý sa začal v roku 2018 oznámením Európskej komisie „Umelá inteligencia pre Európu“ a zriadením Expertnej skupiny na vysokej úrovni pre umelú inteligenciu. Na základe etických pokynov a odporúčaní vypracovaných touto skupinou prijala Komisia vo februári 2020 Bielu knihu o Umelej inteligencii, po ktorej nasledovala verejná konzultácia s viac ako 1 000 príspevkami.

Globálny Hub

Hlavným politickým cieľom návrhu je zmeniť Európu na globálne centrum (hub) dôveryhodnej UI a dosiahnuť rovnováhu medzi budovaním dôvery občanov v systémy umelej inteligencie a podporou inovácií a investícií do ďalšieho vývoja. Podľa vzoru všeobecného nariadenia o ochrane údajov (GDPR) sa Komisia sústredila na napojenie nového súboru pravidiel na základné hodnoty EÚ, navrhovanie, vývoj a používanie systémov umelej inteligencie bude musieť byť s nimi v súlade.

Prístup založený na hodnotení rizika

Komisia prijala prístup založený na hodnotení rizika, ktorý vychádza z konceptu: „čím vyššie je riziko, tým prísnejšie je pravidlo“. Návrh preto rozdeľuje systémy umelej inteligencie do štyroch kategórií:

Kategória rizika	
Neprijateľné riziká	Systémy umelej inteligencie spadajúce do tejto kategórie sú zakázané, pretože sa považujú za systémy, ktoré sú v rozpore so základnými právami a hodnotami EÚ. Medzi zakázané systémy umelej inteligencie budú patriť také, ktoré používajú manipulatívne praktiky, napríklad praktiky, ktoré majú značný potenciál manipulovať s ľuďmi pomocou podprahových metód a ďalej sociálny bodový systém vykonávaný verejnými autoritami (social scoring).
Vysoké riziká	<p>Vysoko rizikové systémy umelej inteligencie budú povolené, iba ak vyhovujú určitým povinným požiadavkám, ktoré zahŕňajú správu údajov, vedenie dokumentácie a záznamov, transparentnosť a poskytovanie informácií používateľom, ľudský dohľad, robustnosť, presnosť a bezpečnosť, ako aj ex-ante posudzovanie zhody.</p> <p>Identifikácia vysoko rizikových systémov umelej inteligencie bude súvisieť s ich zamýšľaným účelom a bude zahŕňať systémy používané v nasledujúcich sektoroch: kritická infraštruktúra, vzdelávanie, recruiting, nástroje týkajúce sa kontroly hraníc a migrácie, súdnictvo a zložky výkonu práva.</p> <p>Do tejto vysoko rizikovej skupiny zahrnula Komisia aj biometrické systémy používané v reálnom čase (napr. rozpoznávanie tváre), ktoré budú zakázané, avšak s výnimkami, t.j. bude povolené ich používať ak to bude odôvodnené špecifickými dôvodmi - pátranie po nezvestnom dieťati, zabránenie konkrétnej a bezprostrednej teroristickej hrozbe alebo na lokalizáciu podozrivých zo závažného trestného činu. Toto už bolo kritizované z pohľadu ochrany osobných údajov v spoločnom stanovisku Európskeho dozorného úradníka pre ochranu údajov a Európskeho výboru pre ochranu údajov.</p>
Nízke riziká	Systémy umelej inteligencie, na ktoré sa budú vzťahovať iba špecifické povinnosti transparentnosti, aby občania vedeli, že na druhej strane s nimi interaguje stroj (a nie človek), napr. chatovací roboti.
Minimálne riziká	Túto poslednú skupinu tvoria systémy umelej inteligencie, ktoré nepredstavujú riziko ani hrozbu pre základné práva občanov a na ktoré sa nebude vzťahovať žiadna osobitná povinnosť.

Nový dohľad

Pokiaľ ide o správu a riadenie, Komisia navrhuje, aby dohľad nad trhom, vrátane kontroly a hodnotenia, vykonávali príslušné vnútroštátne orgány. Navrhuje sa, že niektorí poskytovatelia systémov umelej inteligencie budú môcť vykonávať aj technické sebahodnotenia. Návrh tiež predpokladá, že bude vytvorená Európska rada pre umelú inteligenciu (European Artificial Intelligence Board) zo zástupcov Komisie a členských štátov, ktorá bude mať vplyv pri určovaní praktických účinkov návrhu Nariadenia. Okrem toho, Komisia bude prevádzkovať celoeurópsku databázu, v ktorej budú poskytovatelia povinní zaregistrovať vysoko rizikové systémy umelej inteligencie, a to ešte pred ich uvedením na trh.

Sporné body

Pokiaľ ide o stret regulácie UI a ochrany súkromia, hlavným sporným bodom bude pravdepodobne použitie systémov UI na účely rozpoznávania tváre. Toto už kritizovali Európsky dozorný úradník pre ochranu údajov a Európsky výbor pre ochranu údajov a niektorí poslanci Európskeho parlamentu budú tiež presadzovať úplný zákaz.

Zainteresované strany tiež poukázali na nejasnosť a nedostatok právnej istoty v súvislosti s niektorými definíciami - definíciou vysoko rizikových systémov umelej inteligencie a definíciou pre podprahové techniky, ktorá je používaná v súvislosti so zakázanými systémami umelej inteligencie.

Z dôvodu nejasného znenia v **recitáli 9** je ďalšou otvorenou otázkou, či sa nové pravidlá budú vzťahovať na systémy umelej inteligencie, ktoré sú zabudované do online platforiem. **Kľúčoví** vývojári a používatelia umelej inteligencie budú chcieť zaistiť, aby postup hodnotenia rizika nebol pre nich príliš zaťažujúci.

Aspekty právnej zodpovednosti spojené s navrhovaním, vývojom a používaním systémov **UI** nepatria do rozsahu pôsobnosti návrhu Nariadenia, hoci Európsky parlament pôvodne požadoval režim občianskoprávnej zodpovednosti za **UI**. Očakáva sa, že Komisia sa bude zaoberať aspektmi zodpovednosti súvisiacimi s novými technológiami v rámci pripravovanej rozsiahlejšej revízie právneho rámca zodpovednosti.

Ďalšie kroky

Nariadenie o umelej inteligencii prejde riadnym legislatívnym postupom EÚ a stane sa záväzným pre členské štáty, až keď ho prijme Európsky parlament aj Rada. Komisia plánuje, že Nariadenie by malo byť uplatniteľné rok a pol po jeho prijatí, s tým, že Rada pre umelú inteligenciu by mala byť funkčná už skôr.

2. Nariadenie o umelej inteligencii z pohľadu ochrany osobných údajov

K návrhu [Nariadenia, ktorým sa ustanovujú harmonizované pravidlá umelej inteligencie](#) („Nariadenie o UI“) vydali už svoje spoločné stanovisko Európsky dozorný úradník pre ochranu údajov (European Data Protection Supervisor - EDPS) a Európsky výbor pre ochranu údajov (European Data Protection Board - EDPB). Hoci toto stanovisko nie je pre Komisiu záväzná, EDPS a EDPB sú priamo zodpovední za presadzovanie pravidiel ochrany údajov, a preto je pravdepodobné, že ich názory budú mať vplyv na európske inštitúcie.

Stanovisko všeobecne víta úsilie Komisie o reguláciu umelej inteligencie (UI), ako aj zvolený prístup založený na riziku, avšak zároveň poukazuje na niekoľko aspektov navrhovaného Nariadenia o UI, ktoré by sa mali zmeniť a doladiť, obzvlášť pokiaľ ide o stret s európskym právnym rámcom ochrany údajov.

V prvom rade sa v stanovisku požaduje všeobecný zákaz „akéhokoľvek použitia umelej inteligencie na automatické rozpoznávanie ľudských znakov na verejne prístupných miestach v akomkoľvek kontexte“. Podľa európskeho dozorného úradníka pre ochranu údajov Wojciecha Wiewiórowského by takýto zákaz predstavoval „nevyhnutný východiskový bod, ak chceme zachovať naše slobody a vytvoriť právny rámec pre umelú inteligenciu zameranú na človeka“. Pripomíname, že Nariadenie o UI v tomto ohľade neobsahuje úplný zákaz, ale obsahuje zoznam výnimočných prípadov, keď je zo stanovených dôvodov povolená vzdialená biometrická identifikácia vo verejnom priestore v reálnom čase.

EDPS a EDPB sa domnievajú, že prístup Komisie je v rozpore so zásadou proporcionality, pretože by bolo potrebné spracovať obrovské množstvo údajov, aby bolo možné identifikovať iba niekoľko jednotlivcov. Takýto proces by navyše mal nezvratné účinky na slobodu pohybu, prejavu, zhromažďovania a združovania občanov.

Z pohľadu EDPS a EDPB je tiež nevyhnutný zákaz systémov UI kategorizujúcich jednotlivcov na základe biometrie do skupín (klastrov) podľa etnického pôvodu, pohlavia, politickej alebo sexuálnej orientácie alebo iných diskriminačných dôvodov zakázaných v Charte ľudských práv EÚ. Podľa EDPS a EDPB takzvaná „biometrická kategorizácia“ upravená v Nariadení predstavuje riziko pre ľudskú dôstojnosť, pretože budúce správanie jednotlivcov sa nebude hodnotiť podľa ich vlastnej vôle, ale bude kategorizované počítačom.

Pokiaľ ide o správu a riadenie, v stanovisku sa zdôrazňuje potreba jasne stanoviť nezávislú povahu orgánov, ktoré budú plniť úlohu dohľadu. V tejto súvislosti EDPS a EDPB požadujú väčšiu autonómiu pre Európsku radu pre umelú inteligenciu (European Artificial Intelligence Board - EAIB). Podľa súčasného návrhu by mala mať v EAIB významnú úlohu samotná Komisia, pričom EDPS a EDPB zastávajú názor, že toto by to mohlo narušiť nezávislosť rady, najmä pokiaľ ide o vonkajšie politické vplyvy. Namiesto toho by sa rade malo umožniť, aby konala z vlastnej iniciatívy.

S cieľom zabezpečiť vyššiu harmonizáciu v rámci legislatívneho rámca EÚ a lepšiu koordináciu medzi Nariadením o umelej inteligencii a predpismi EÚ týkajúcimi sa ochrany osobných údajov sa v stanovisku navrhuje, aby zodpovednými orgánmi podľa článku 59 návrhu Nariadenia, boli vnútroštátne orgány na ochranu údajov, keďže tieto už sú zodpovedné za vykonávanie ustanovení týkajúcimi sa ochrany osobných údajov v systémoch umelej inteligencie, ktoré spracúvajú osobné údaje. V stanovisku sa uvádza, že tento režim riadenia by bol prospešný pre všetky subjekty zapojené do riešenia otázok ohľadom UI, pretože budú mať jednotné kontaktné miesto pre všetky operácie a spory týkajúce sa spracovania údajov.

Na záver sa stanovisko zameriava na certifikáciu systémov UI, pričom sa domnieva, že tu chýba jasný vzťah s pravidlami EÚ na ochranu údajov. Uvádza sa v ňom, že súčasný systém navrhnutý v návrhu Nariadenia o UI by mal byť lepšie zosúladený s certifikáciami o ochrane údajov stanovenými v GDPR. V opačnom prípade môže vzniknúť riziko, že na trh EÚ budú uvedené výrobky, ktoré sú síce certifikované podľa Aktu o umelej inteligencii, avšak nie sú v súlade s pravidlami a zásadami ochrany údajov. V stanovisku sa predovšetkým navrhuje, aby sa pri vydávaní certifikácie podľa Nariadenia o umelej inteligencii zohľadňovali zásady minimalizácie údajov.

Stanovisko EDPB a EDPS opäť zdôrazňuje zložitosť uvedenej problematiky a potenciál rozporov s existujúcimi právnymi predpismi EÚ, a je zrejmé, že o návrhu budú ešte pred jeho prijatím prebiehať intenzívne rokovania.

3. Ochrana spotrebiteľov v online prostredí

Podľa Európskej Komisie online nakupovanie v dôsledku pandémie Covid-19 výrazne vzrástlo. V roku 2020 nakupovalo online až 71% európskych spotrebiteľov, čo vyzdvihlo aktuálnu potrebu nových právnych predpisov, ktoré majú ísť nad rámec pôvodných pravidiel bezpečnosti tovarov a sú viac prispôbené online prostrediu.

Tento návrh nariadenia je v súlade s novou agendou spotrebiteľov z roku 2020 zameranou na aktualizáciu a modernizáciu všeobecného rámca pre bezpečnosť nepotravinárskych spotrebných výrobkov s cieľom zachovať úlohu bezpečnostnej siete pre spotrebiteľov a prispôbiť právny rámec výzvam spojeným s online predajom. Návrhom by sa mala nahradiť smernica 2001/95/ES o všeobecnej bezpečnosti tovarov.

Povinnosti a pokuty

Podľa navrhovaných nových pravidiel budú regulačné orgány schopné nariadiť online trhoviskám, aby do dvoch dní odstránili nebezpečné výrobky, zakázali k nim prístup alebo upozornili spotrebiteľov cez „výslovné varovanie“ v prípade, že nebudú podniknúť prvé dva kroky. Ak spoločnosti uvedenú povinnosť nedodržia, môže im byť udelená pokuta až vo výške 4% ročného obratu spoločnosti. Podľa nových pravidiel by spoločnosti mali konať bez zbytočného odkladu, keď sa na ich platformu dostane nebezpečný produkt.

Návrh tiež obsahuje podmienky, za ktorých by sa využívali údaje o zákazníkoch, ktoré majú spoločnosti k dispozícii, na informovanie spotrebiteľov o stiahnutiach z trhu a o bezpečnostných varovaniach. Oznámenie o stiahnutí z trhu by malo byť jasné, transparentné a zreteľne popisujúce príslušné riziko, pričom bude potrebné sa vyhýbať akýmkoľvek výrazom alebo iným prvkom, ktoré by mohli znížiť vnímanie rizika spotrebiteľmi.

Vzťah k Aktu o digitálnych službách

Revízia má tiež doplniť navrhovanú reguláciu v Akte o digitálnych službách (Digital Services Act - DSA), o ktorom sa v súčasnosti rokujú na úrovni EÚ a ktorý obsahuje aj nové povinnosti sprostredkovateľov služieb pre spotrebiteľov v online priestore. Pripomínáme, že jednou z požiadaviek, ktoré sa majú presadzovať v rámci DSA, sú pravidlá týkajúce sa sledovateľnosti podnikateľov na online trhoviskách, aby sa zabezpečila identifikácia predajcov nelegálneho tovaru. Nový návrh tiež znamená, že predajcovia na online trhovisku musia spotrebiteľovi poskytnúť určité informácie, napríklad meno výrobcu, registrovanú ochrannú známku a miesto podnikania.

Ďalšie kroky

Čo sa týka aktuálneho stavu, návrh musí byť ešte prerokovaný Európskym parlamentom a členskými štátmi v Rade EÚ. Po jeho prijatí, vstúpi v platnosť dvadsiatym dňom po jeho uverejnení v Úradnom vestníku Európskej únie. Uplatňovať sa začne následne, po šiestich mesiacoch odo dňa nadobudnutia platnosti. Toto nariadenie bude priamo uplatniteľné vo všetkých členských štátoch EÚ.

4. Akt o údajoch („Data Act“)

Povinnosť pre súkromné spoločnosti umožniť prístup k údajom podľa plánovaného EU návrhu

Súkromné spoločnosti by mohli čeliť povinnosti umožniť novým účastníkom trhu prístup k ich údajom, a to podľa nových pravidiel navrhovaných Európskou Komisiou vo forme Aktu o údajoch, ktorý by mal byť publikovaný neskôr tento rok. Počiatočné náhľady do tohto plánu sú poskytnuté v nedávnej publikácii – Počiatočné posúdenie dopadov („[Inception Impact Assessment](#)“), ktorá umožňovala všetkým zúčastneným stranám poskytnúť spätnú väzbu k zamýšľanému návrhu.

Budúci Akt o údajoch má slúžiť na vytvorenie jednotného digitálneho trhu, v ktorom údaje prúdia medzi krajinami a sektormi a kde existujú férové, praktické a jasné pravidlá pre prístup a použitie údajov. Mal by mať formu horizontálnej legislatívnej iniciatívy, dopĺňajúcej návrh Nariadenia o Európskej správe údajov, ktorý bol zverejnený minulý rok a v súčasnosti sa o ňom rokuje. Cieľom by bolo ďalšie uľahčenie prístupu k údajom a zdieľanie údajov v prospech startupov a malých a stredných podnikov.

Vychádzajúc zo skúseností s pandemiou, keď sa rozhodnutia vlád zakladali na dostupných údajoch, návrh by mal tiež podporiť prístup a používanie veľkých zdrojov údajov (big data) súkromných spoločností, čo by mohlo viesť k rýchlejšim a cielenejším reakciám na spoločenské zmeny. Okrem iných cieľov, iniciatíva by sa mala snažiť tiež o zlepšenie prenosu údajov medzi cloudovými službami v celej dátovej ekonomike. Okrem toho, existujúca Smernica o právnej ochrane databáz by mohla byť zmenená tak, aby podporovala ciele tejto iniciatívy.

Na druhú stranu spoločnosti, ktoré generujú proprietárne dáta, môžu byť znepokojené návrhom novej legislatívy oslabujúcej ich investície a potenciálne ohrozujúcej ich obchodné tajomstvá. Taktiež vzniká obava, že Akt o údajoch môže odobrať určité privilegované postavenie niektorých spoločností, obzvlášť výrobcov objektov pripojených na internet a ohroziť investície do objektov generujúcich údaje.

V súčasnosti Komisia zvažuje nasledujúce politické možnosti:

- **Zlepšený prístup k údajom súkromného sektora pre verejný sektor:** toto by mohlo zahŕňať navrhnutie flexibilnejšieho rámca pre prístup a použitie údajov, vrátane požiadaviek na zdieľanie údajov, transparentnosť a bezpečnosť. Jednou z možností, ktorá by však mohla byť kontroverzná, by bolo zakotvenie práva verejného sektora na prístup k súkromným údajom pre zadané účely vo verejnom záujme.
- **Zabezpečenie férovosti prístupu k údajom a ich použitiu v B2B situáciách:** Možnosti na zváženie zahŕňajú:
 - 1 Špecifické povinnosti transparentnosti pre výrobcov pripojených objektov týkajúce sa práv prístupu a použitia neosobných údajov pre profesionálne účely v prospech používateľov takých objektov;
 - 2 B2B test férovosti, aby sa predišlo jednostranne zavedeným neférovým podmienkam pre prístup a použitie údajov. Taký test by mohol byť implementovaný modelovými zmluvnými podmienkami odporúčanými Komisiou;
 - 3 Úprava práv na prístup a použitie údajov, založená na férových, vhodných, primeraných, transparentných a nediskriminačných (FRAND) podmienkach pre neosobné údaje. Toto by sa mohlo tiež vzťahovať na špecifické údaje, ako sú neosobné údaje generované objektmi IoT;
 - 4 Poskytovanie horizontálnych prostriedkov pre prístup k údajom, napríklad na základe podmienok „FRAND“, ktoré by sa mohli vzťahovať na práva prístupu k údajom vytvoreným v rámci špecifických sektorových pravidiel, berúc do úvahy špecifické charakteristiky relevantného trhu napr. pravidlá o údajoch vo vozidle;

5 Preskúmanie úlohy súčasných práv a výnimiek na základe existujúcej Smernice o právnej ochrane databáz, aby sa zabezpečilo, že sa nevytvára prekážka v prístupe k údajom a ich použitiu, obzvlášť pokiaľ ide o strojovo vytvorené údaje a údaje vytvorené v kontexte internetu vecí (Internet of Things, IoT).

- **Prispieť k prenosnosti údajov vytvorených jednotlivcami:** Právny nástroj by poskytol technické špecifikácie, aby pomohol jednotlivcom získať výhody práva na prenos v zmysle Všeobecného nariadenia o ochrane osobných údajov (GDPR). Mohol by poveriť spoločnosti predávajúce prostriedky pre smart domácnosť, wearables, domácich asistentov, aby umožnili v skutočnom čase prenos údajov, ktoré tieto zariadenia zhromažďujú počas ich používania.
- **Zabezpečenie súťažného cloudového trhu umožnením ľahkého prenosu cloudových služieb:** Akt o údajoch by mohol uložiť poskytovateľom cloudových služieb záväznú povinnosť ponúknuť prenos údajov a aplikácií. Rôzne scenáre by mohli zahŕňať:
 - 1 Obmedzenie intervencie len na úpravu v štandardných zmluvných doložkách, vyvinutých na základe Kódexov Správania, ktoré už odvetvie poskytlo;
 - 2 Formulovanie základných právnych požiadaviek v Akte o údajoch, pre všetkých poskytovateľov cloudových počítačových služieb na trhu;
 - 3 Rozvoj špecifických právnych požiadaviek definujúcich podmienky zmluvnej, technickej a ekonomickej povahy.
- **Zadefinovať nevyhnutné podmienky pre interoperabilitu smart kontraktov,** ktoré by mohli dopĺňať prípadný mandát pre Európsky výbor pre normalizáciu na vytvorenie technických štandardov pre smart kontrakty.
- **Znížiť riziká vyplývajúce z vládneho prístupu k neosobným údajom spoločností založených v Únii,** ktoré sú v dispozícii poskytovateľov cloudových služieb a zabezpečenie dôvery v používanie cloudových služieb - zvažujú sa nasledujúce možnosti:
 - 1 Pre poskytovateľov cloudových služieb stanoviť povinnosť notifikovať používateľa (v rozsahu povolenom podľa príslušného cudzieho práva), a to zakaždým, keď obdržia žiadosť o prístup k údajom od zahraničnej authority, ako aj povinnosť oznámiť Komisii všetky cudzie predpisy s extra-teritoriálnym dosahom, ktorým podliehajú. Tieto informácie by mali byť zverejnené na Portáli Transparentnosti EU.
 - 2 Prvá možnosť a, k nej navyše, poveriť cloudových poskytovateľov, aby zabezpečili implementáciu vhodných právnych, technických a organizačných opatrení, aby sa zabránilo prenosu alebo prístupu k neosobným údajom spoločností založených v Únii a v dispozícii cloudových poskytovateľov, a to vládnym autoritám z tretích krajín, kde by taký prenos alebo prístup mohol byť v rozpore s právom EU alebo lokálnymi predpismi.

Ďalšie kroky

Počiatočné posúdenie dopadov („Inception Impact Assessment“) bolo otvorené pre prijatie spätnej väzby od zúčastnených strán do 25. júna. Reakcie na konzultačný proces, zhromažďovanie dôkazov a konečné výsledky prebiehajúcej štúdie o férovosti v zdieľaní údajov a prístupe k údajom, budú zohľadnené v konečnom návrhu Akte o údajoch, ktorý by mal byť zverejnený v treťom alebo štvrtom kvartáli 2021.

5. Akt o digitálnych trhoch („Digital Markets Act“) – návrhy od BEREC

Prostriedky nápravy navrhnuté na mieru a zapojenie ďalších subjektov

Orgán európskych regulátorov pre elektronické komunikácie (BEREC) prispel k prebiehajúcej debatae o navrhovanom Akte o digitálnych trhoch (DMA) a zverejnil tri návrhy poskytujúce náhľad na potenciálny dopad návrhu DMA na telekomunikačný trh.

Vo svojom návrhu o prostriedkoch nápravy navrhnutých na mieru a štruktúrovaných procesoch účasti pre zúčastnené strany, sa BEREC zameriava na skúsenosti národných regulačných autorít pri regulácii telekomunikačných trhov. BEREC verí, že navyše k priamo uplatniteľným povinnostiam, DMA návrh by mohol obsahovať aj súbor ex ante princípov a nápravných opatrení („toolbox“). Toto by poskytlo Európskej komisii, ako kompetentnému orgánu na úrovni EÚ, možnosť navrhovať prostriedky nápravy na mieru tak, aby sa dosiahol cieľ regulácie.

Skúsenosti s analýzou trhu v sektore elektronických komunikácií ukázali, že prístup, ktorý je založený na princípoch, umožňuje analýzu, prijatie a úplnú implementáciu opatrení na vhodné dosiahnutie cieľov rýchlejšie ako pri priamo aplikovateľnej regulácii. Okrem toho, staticky upravené povinnosti nemusia byť postačujúce v budúcnosti.

Podľa BEREC, DMA by mal uľahčiť ukladanie prostriedkov nápravy na mieru, ktoré sú z dlhodobého hľadiska efektívnejšie a rýchlejšie riešia identifikované problémy, keďže poskytujú nevyhnutnú flexibilitu na prispôsobenie regulačných opatrení špecifickým „strážcom prístupu“ („gatekeeper“), službe alebo situácii na trhu. BEREC vníma potrebu pre použitie ex ante princípov, ktoré by sa uplatňovali na prispôsobenie všeobecných prostriedkov nápravy (akými sú prístup, interoperabilita a nediskriminácia), vykonávaných prostredníctvom Komisie a podporovaných národnými nezávislými autoritami.

BEREC ďalej považuje za veľmi dôležité, aby DMA poskytoval transparentnosť a umožnil prostredníctvom riadnej procedúry štruktúrovanú účasť všetkých dotknutých strán poskytujúcich ich stanoviská, a nie iba regulovaných entít. BEREC zvažuje, že ďalšie zúčastnené tretie strany, ako biznis užívatelia alebo alternatívne platformy, by mali byť vhodne zapojené do procesu, aby bola zaistená transparentnosť a nestrannosť.

Navyše, namiesto implementačného zákona, BEREC navrhuje, aby DMA predpokladal zverejnenie usmernení založených na súbore princípov alebo prvkov, ktoré by mali byť zahrnuté vo všetkých dohodách medzi platformami ako tzv. strážcami prístupu („gatekeeper“) a biznis používateľmi.

Zriadenie Poradného výboru

BEREC tiež zverejnil návrh na zriadenie Poradného Výboru v kontexte DMA. BEREC poznamenal, že DMA počíta s centrálnou úlohou pre Európsku komisiu a medzivládny výbor a okrem výboru sa nepredpokladá ďalšia národná intervencia, ktorá by podporovala Komisiu pri vykonávaní ustanovení DMA. BEREC vidí význam v poskytovaní podpory od národných nezávislých autorít pri vykonávaní ustanovení DMA prostredníctvom Poradného výboru pre:

- a priznanie vplyvu DMA pre malých „hráčov“;
- b umožnenie konštantného monitoringu s dostatočnou presnosťou;
- c zabezpečenie dostatočných špecializovaných zdrojov s relevantnou technickou expertízou podporujúcou presadzovanie DMA Komisiou;
- d zabezpečenie toho, že rozhodnutia Komisie sú založené na existujúcich a náležitých skúsenostiach;

- e podporu Komisie v procesoch riešenia sporov, a;
- f zabezpečenie konzistentnosti s doplňujúcou reguláciou.

Vzájomné pôsobenie s interpersonálnymi komunikačnými službami nezávislými na číslach

V [správe](#) o vzájomnom pôsobení medzi Európskym kódexom elektronických komunikácií („Kódex“) a DMA návrhom týkajúcej sa interpersonálnych komunikačných služieb nezávislých na číslach, BEREC zdôraznil potrebu vyhnúť sa potenciálnemu regulačnému prekryvaniu, odporujúcim si prostriedkom nápravy a právnej neistote. V tomto kontexte sa zvažuje, že takáto kolízia s reguláciou elektronických komunikácií by sa mala riešiť uprednostnením opatrení v rámci existujúceho regulačného rámca (t.j. Kódexu).

Okrem toho, BEREC navrhuje rad zmien na lepšie riešenie potenciálneho súbežného prekrytia medzi DMA a Kódexom. Cieľom je objasniť, že DMA nezahŕňa a ani nebude zahŕňať žiadne základné platformové služby iné ako interpersonálne komunikačné služby nezávislé na číslach poskytované strážcami prístupu („gatekeepers“). Všetky právomoci obsiahnuté v Kódexe zostávajú uplatniteľné na také služby. Mechanizmus spolupráce by mal byť implementovaný medzi Komisiou, BEREC-om, národnými regulačnými autoritami a/alebo budúcim DMA Poradným výborom.

Ďalšie kroky

Keďže BEREC nemá k dispozícii inštitucionálne prostriedky, aby sa mohol zapojiť do legislatívneho procesu, zostáva len sledovať, či Komisia, Výbor ministrov a Európsky parlament prijmú v konečnej podobe Aktu o digitálnych trhoch návrhy BEREC.

6. Verejné konzultácie

Názov	Termín
Európska vízia Digitálnej Dekády 2030	3.8.2021
Označovanie energetickej účinnosti mobilných telefónov a tabletov – informovanie spotrebiteľov o vplyve na životné prostredie	23.8.2021
Smernica o všeobecnej bezpečnosti výrobkov - preskúmanie	21.9.2021
Digitálny identifikačný systém EÚ pre elektronické transakcie v celej Európe	02.09.2021
Vyhlásenie o digitálnych zásadách – európsky spôsob digitálnej spoločnosti	02.09. 2021
Akt o údajoch a novelizované predpisy o právnej ochrane databáz	03.09.2021

Kontaktujte nás:

Ivan Kisely

Counsel

Tel: +421232332825
ivan.kisely@twobirds.com



Katarína Ondrovičová

Seniorná advokátka

Tel: +421232332819
katarina.ondrovicova@twobirds.com



Zuzana Juričková

Advokátka

Tel: +421232332816
zuzana.jurickova@twobirds.com



Robert Čuperka

Advokátsky koncipient

Tel: +421232332814
robert.cuperka@twobirds.com



twobirds.com

Abu Dhabi & Amsterdam & Bratislava & Brusel & Budapešť & Kodaň & Dubaj & Düsseldorf & Frankfurt & Haag & Hamburg & Helsinki & Hong Kong & Londýn & Luxemburg & Lyon & Madrid & Miláno & Mníchov & Paríž & Peking & Praha & Rím & San Francisco & Šanghai & Singapur & Štokholm & Sydney & Varšava & Pridružená kancelária: Casablanca

Bird & Bird je medzinárodná advokátska kancelária skladajúca sa z Bird & Bird LLP a jej pobočiek a pridružených zastúpení. Bird & Bird LLP je registrované v Anglicku a Walse pod registračným číslom OC340318 a je regulované SRA – Regulačnou autoritou. Jej sídlom a miestom podnikania je 12 New Fetter Lane, Londýn, EC4A 1JP. Zoznam členov skupiny Bird & Bird LLP a nečlenov, ktorí sú vymenovaní za partnerov a ich príslušné odborné kvalifikácie, sú k dispozícii k nahliadnutiu na tejto adrese.