

Bird & Bird & Aktuality z EÚ legislatívy

Január 2021

V tomto vydaní Aktualít z EÚ legislatívy prinášame stručný prehľad pracovného programu Európskej Komisie na rok 2021 a kľúčových iniciatív, ktoré Komisia plánuje prijať v tomto roku. V centre jej programu bude digitálna a zelená transformácia. Prinášame tiež základné informácie o navrhovanej zmene v súčasnosti platných, a len nedávno schválených pravidiel kybernetickej bezpečnosti. Na záver predkladáme zhrnutie návrhu o online teroristickom obsahu a zoznam aktuálne prebiehajúcich verejných konzultácií. Naďalej pre vás monitorujeme legislatívny proces týkajúci sa tzv. Digitálneho balíka – Digital Services Act a Digital Markets Act a bližšie informácie prinesieme v ďalších vydaniach Aktualít z EÚ legislatívy.

Obsah:

1 [Pracovný program Komisie na 2021](#)

2 [Kybernetická bezpečnosť](#)

3 [Online teroristický obsah](#)

4 [Verejné konzultácie](#)

1. Pracovný program Komisie na 2021

Digitálna a zelená transformácia ako top priority na rok 2021

Digitálna a zelená transformácia, boli v centre nedávno prezentovaného pracovného programu Európskej Komisie na rok 2021. Tento program stanovuje kľúčové iniciatívy, ktoré Komisia plánuje prijať v tomto roku a zároveň stanovuje priority nevybavenej legislatívy a stiahnutie určitých návrhov. Európska Komisia uviedla: „*pandémia zvýraznila potrebu, aby Európa stála v čele súbežnej zelenej a digitálnej transformácie a zvýšila odolnosť svojich spoločností a hospodárstiev*“. V komunikácii sa tiež uvádza, že 20% dočasného núdzového plánu obnovy, označeného ako NextGenerationEU, sa investuje do digitálnej transformácie.

Komisia potvrdila, že viaceré prioritné iniciatívy z roku 2020 musia byť dokončené, vrátane viacerých návrhov Digitálno-finančného balíka a e-Privacy nariadenia. Jej nový pracovný program pre rok 2021 je rozdelený do nasledujúcich šiestich kapitol, ktoré odzrkadľujú politické usmernenia Komisie pod vedením Ursuly von der Leyen:

- 1 Európska Zelená dohoda;
- 2 Európa pripravená na digitálny vek;
- 3 Hospodárstvo, ktoré pracuje v prospech ľudí;
- 4 Silnejšia Európa vo svete;
- 5 Podpora európskeho spôsobu života; a
- 6 Nový impulz pre európsku demokraciu.

Digitálny segment obsahuje 9 akčných bodov, z ktorých 6 by malo obsahovať jeden alebo viac legislatívnych návrhov:

• Digitálna dekáda Európy

Ide o nelegislatívny návrh, ktorým Komisia stanovuje ciele v rôznych oblastiach, ako je konektivita, digitálne zručnosti a digitálne verejné služby. V tomto kontexte už Komisia vydala Odporúčania zvýšiť investície do vysoko kapacitnej široko pásmovej infraštruktúry, vrátane 5G. Taktiež navrhuje nadväzujúcu reguláciu pre európske spoločné podniky pre vysoko výkonné výpočtové systémy s investíciou 8 miliónov eur do ďalšej generácie superpočítačov.

• Dátový balík

Dátový balík obsahuje predovšetkým zákon o údajoch (Data Act) a revíziu smernice o databázach. Obidva návrhy sa očakávajú v treťom štvrtroku 2021. Zákon o údajoch stanoví podmienky pre zdieľanie a kontrolu údajov zo strany občanov, podnikov a štátnych orgánov. Komisia si taktiež stanovila cieľ revidovať smernicu o databázach z roku 1996.

• Digitálny odvod

Komisia potvrdila svoj zámer pokračovať v presadzovaní medzinárodnej dohody o digitálnom zdaňovaní. Ak k presadeniu medzinárodnej dohody nedôjde, bolo rozhodnuté pokračovať s vlastnými digitálnymi zdaňovacími plánmi. Návrh je naplánovaný na druhý štvrtrok roka 2021.

- **Európska e-Identita**

Komisia navrhla novú európsku digitálnu identitu, aby občanom uľahčila vykonávanie úloh a prístup k službám online naprieč Európou, ako aj aby uistila ľudí, že majú väčšiu kontrolu nad zdieľanými údajmi a tým ako sú použité.

- **Pracovníci platforiem**

Komisia by mala regulovať pracovné podmienky a sociálnu ochranu pracovníkov platforiem prostredníctvom legislatívneho návrhu.

- **Priemyselná stratégia**

Komisia zaktualizuje Priemyselnú stratégiu pre Európu prezentovanú v marci 2020 tak, aby zohľadnila dopady pandémie COVID-19, kontext globálnej súťaže a akceleráciu zelenej a digitálnej transformácie.

- **Zahraničné dotácie**

V snahe vytvoriť spravodlivejšie podnikateľské prostredie, Komisia navrhne jednu alebo viac legislatívnych iniciatív na zabezpečenie rovnakých podmienok a posilnenie presadzovania, pokiaľ ide o zahraničné dotácie narúšajúce európsky trh. Toto nadväzuje na Bielu knihu zverejnenú v júni 2020, ktorá obsahuje viaceré povinnosti pre podniky, ktoré dostali finančné príspevky od štátov, ktoré nie sú v EÚ.

- **Synergia medzi občianskym, obranným a vesmírnym priemyslom**

Akčný plán o synergii medzi týmito odvetvami by mal byť predložený v prvom štvrtroku 2021.

- **Spotrebiteľské práva v oblasti elektroniky**

Komisia plánuje návrh týkajúci sa nových požiadaviek na dizajn a práva spotrebiteľov v oblasti elektroniky, a to koncom roka 2021, zameraný na otázky tzv. zabudovaného zastarávania výrobkov.

Komisia taktiež zaviedla zoznam REFIT iniciatív, ktoré by mali aktualizovať a zjednodušiť existujúce regulácie. Tento zoznam zahŕňa viaceré usmernenia súťažného práva, ako je definícia trhu a viaceré usmernenia o štátnej pomoci.



2. Kybernetická bezpečnosť

Európska Komisia navrhuje aktualizovať Smernicu NIS, a to len dva roky po jej implementácii

Po vznesenej kritike uplatňovania a rozsahu Smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (tzv. Smernica NIS), Európska komisia zverejnila v decembri 2020 [návrh](#) na jej preskúmanie pod označením „Smernica NIS2“. Ako už názov napovedá, cieľom Smernice NIS2 bude aktualizovať súčasnú [Smernicu NIS](#), hoci táto smernica sa v členských štátoch začala uplatňovať až od 9. mája 2018.

Súčasná Smernica NIS, známa tiež ako smernica o kybernetickej bezpečnosti, obsahuje ciele pravidlá (napr. povinnosť oznamovať porušenie) pre prevádzkovateľov základných služieb (poskytovatelia v oblasti energetiky, dopravy, bankovníctva a financií, zdravotníctva, dodávok vody a digitálnej infraštruktúry) a poskytovateľov digitálnych služieb (najmä poskytovatelia online trhoviska, služieb internetových vyhľadávačov a služieb cloud computingu). Členské štáty boli tiež povinné, aby zriadili tím pre riešenie počítačových bezpečnostných incidentov (tzv. CSIRT - computer security incident response team) a príslušný vnútroštátny orgán.

Rozsah pôsobnosti

Cieľom navrhovanej Smernice NIS2 je **zrušiť rozdiel medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb** a preskúmať **nový prístup ku klasifikácii založený na dôležitosti služby**. To by umožnilo ľahší režim pre služby, ktoré sú kategorizované ako „dôležité“, a nie „základné“.

Kategorizácia na základné a dôležité služby sa zakladá na nižšie uvedených sektoroch, ale samotné pôsobenie v jednom z týchto sektorov nebude jediným kritériom, služba musí byť tiež špecifického typu uvedeného v prílohe k návrhu (v ktorom sa stanovuje typ subjektu detailnejšie):

Základná služba

- Energetika
- Doprava
- Bankovníctvo
- Infraštruktúra finančného trhu
- Zdravotníctvo
- Pitná voda
- Odpadová voda
- Digitálna infraštruktúra
- Verejná správa
- Vesmírna oblasť

Dôležitá služba

- Poštové a kuriérske služby
- Odpadová správa
- Chemická výroba, produkcia a distribúcia
- Potravinárska produkcia, spracovanie a distribúcia
- Výroba
- Digitálni poskytovatelia

Je potrebné poznamenať, že poskytovatelia cloudových služieb prešli na vyššiu úroveň základných služieb (v kategórii „digitálna infraštruktúra“), zatiaľ čo zostávajúce kategórie poskytovateľov digitálnych služieb (spadajúci pod „dôležité“) boli rozšírené o poskytovateľov platforiem služieb sociálnych sietí. **Cieľom nového návrhu je teda rozšíriť rozsah pôsobnosti súčasnej smernice NIS pridaním nových odvetví na základe ich kritickosti pre hospodárstvo a spoločnosť.**

Zavádza tiež obmedzenie podľa veľkosti, čo bude znamenať, že **do rozsahu pôsobnosti NIS2 budú zahrnuté iba stredné a veľké spoločnosti** vo vybraných odvetviach, pričom sa zachová určitá flexibilita pre členské štáty pri identifikácii menších subjektov s profilom vysokého bezpečnostného rizika. Toto vyňatie menších spoločností sa však nebude uplatňovať univerzálne, napríklad ak bude poskytovateľom základnej alebo dôležitej služby poskytovateľ verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb.

Rozsah jurisdikcie smernice NIS2 bude naďalej určený primárne tým, v ktorom členskom štáte má poskytovateľ svoju hlavnú prevádzkareň. Podľa NIS2 sa bude za hlavnú prevádzkareň považovať miesto, kde sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie rizík kybernetickej bezpečnosti, a nie miesto, kde má poskytovateľ svoje sídlo v EÚ. Ak sa takéto rozhodnutia neprijímajú v žiadnej prevádzkarni v EÚ, za hlavnú prevádzkareň sa bude považovať členský štát, v ktorom majú subjekty prevádzkareň s najvyšším počtom zamestnancov v EÚ; a ak v EÚ žiadne také subjekty nie sú a poskytovateľ ponúka služby v EÚ, potom bude potrebné ustanoviť zástupcu pre účely NIS.

Ďalšie významné zmeny

Návrh posilňuje bezpečnostné požiadavky na spoločnosti, na ktoré sa vzťahujú predmetné pravidlá, a to zavedením princípu riadenia rizík (technické a organizačné opatrenia) a zároveň poskytuje minimálny **zoznam základných bezpečnostných prvkov**, ktoré sa musia uplatniť. Uvedené si bude vyžadovať normatívnejší prístup, ako sa aktuálne uplatňuje podľa súčasnej smernice NIS. Návrh taktiež zavádza **presnejšie požiadavky na hlásenie incidentov**, vrátane obsahu hlásení a časových harmonogramov hlásenia (v niektorých prípadoch do 24 hodín). Je tiež zaujímavé poznamenať, že cieľom smernice NIS2 je nahradiť konkrétne bezpečnostné požiadavky na poskytovateľov elektronických komunikačných sietí a služieb v Európskom kódexe pre elektronické komunikácie a na poskytovateľov dôveryhodných služieb podľa nariadenia (EÚ) č. 910/2014.

Bezpečnosť dodávateľských reťazcov a dodávateľských vzťahov bola v posledných rokoch obzvlášť horúcou témou a smernica NIS2 vyžaduje, aby jednotlivé spoločnosti riešili riziká kybernetickej bezpečnosti v dodávateľských reťazcoch a dodávateľských vzťahoch.

Vo všeobecnosti platí, že návrh smernice NIS2:

- zavádza prísnejšie opatrenia v oblasti dohľadu pre národné orgány (zachováva požiadavku mať CSIRT);
- obsahuje prísnejšie požiadavky na právnu vymožiteľnosť;
- zlepšuje spoluprácu a zdieľanie informácií medzi členskými štátmi, a to aj prostredníctvom vytvorenia nového orgánu (CyCLONe) pre koordinované riadenie rozsiahlych incidentov a kríz v oblasti kybernetickej bezpečnosti a zabezpečenie pravidelnej výmeny informácií medzi členskými štátmi a orgánmi EÚ; a
- zameriava sa na harmonizáciu sankčných režimov vo všetkých členských štátoch (vrátane pokút do výšky 10 000 000 EUR alebo do 2% z celkového svetového ročného obratu podniku).

Ďalšie kroky

Návrh smernice NIS2 bude predmetom rokovaní medzi Radou a Európskym parlamentom a po jej prijatí budú členské štáty povinné transponovať smernicu NIS2 do 18 mesiacov.

3. Online teroristický obsah

Podľa nových pravidiel má byť teroristický online obsah odstránený do jednej hodiny

Dosiahnutá dohoda

Trojstranné vyjednávania v decembri 2020 medzi Európskou Komisiou, Európskym Parlamentom a Radou konečne dospeli k politickej dohode o návrhu o teroristickom obsahu online. Podľa dohodnutého textu bude teroristický obsah definovaný v súlade so smernicou 2017/541 o boji proti terorizmu.

Základ návrhu je založený na všeobecnom princípe v zmysle, ktorého „to, **čo je nelegálne offline, je nelegálne aj online**“. Vychádzajúc z tejto premisy, môžu byť nové povinnosti pre online platformy, ktoré majú byť zavedené prostredníctvom tejto novej legislatívy, zhrnuté nasledovne:

- Autoritám bude umožnené nariadiť online poskytovateľom služieb odstránenie teroristického obsahu z internetu do jednej hodiny;
- Obsah, ktorý bol chybné stiahnutý, môže byť obnovený;
- Obsah šírený pre edukačné, žurnalistické, umelecké alebo vedecké účely bude vyňatý z pravidla jednej hodiny;
- Požiadavka na odstránenie online teroristického obsahu môže byť adresovaná akýmkoľvek online platformám založeným v EÚ;
- Online platformy budú musieť proaktívne riešiť šírenie teroristického obsahu prostredníctvom ich služieb;
- Online poskytovatelia budú povinní každoročne podávať správy o monitorovaní ich snáh v tejto oblasti.

Po dvoch rokoch diskusií zameraných najmä na zásadnú otázku pravidla jednej hodiny, došlo po nedávnych teroristických útokoch vo Francúzsku, Rakúsku a Nemecku, ku konečnému tlaku smerujúcemu ku konsenzu v tejto citlivej otázke. Legislatívci dospeli k názoru, že tieto udalosti demonštrovali urgentnú potrebu regulovať teroristické aktivity online tak, ako sa to deje aj v offline svete.

Ďalšie kroky

Navrhovaná regulácia musí byť ešte formálne schválená Európskym Parlamentom a Radou, predtým ako oficiálne nadobudne účinnosť.



4. Verejné konzultácie

Tím Bird & Bird je pripravený pomôcť zainteresovaným stranám s odpoveďami na ktorúkoľvek z nasledujúcich verejných konzultácií:

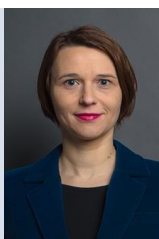
Európska Komisia

Názov	Termín
<u>Spoločné využívanie údajov v EÚ – spoločné európske dátové priestory (nové pravidlá)</u>	1. február 2021
<u>Vysokorýchlostný širokopásmový prístup na internet v EÚ – revízia pravidiel</u>	2. marec 2021
<u>Kybernetická bezpečnosť – preskúmanie pravidiel EÚ týkajúcich sa bezpečnosti sietí a informačných systémov</u>	17. marec 2021
<u>Akt o digitálnych službách – prehĺbenie vnútorného trhu a objasnenie zodpovednosti za digitálne služby</u>	17. marec 2021
<u>Balík, ktorý sa týka aktu o digitálnych službách – regulačný nástroj ex ante zameraný na rozsiahle online platformy, ktoré pôsobia ako strážcovia prístupu</u>	17. marec 2021
<u>Finančné služby – zvýšenie odolnosti proti kybernetickým útokom (nové pravidlá)</u>	17. marec 2021
<u>Ochrana kritickej infraštruktúry v EÚ – nové pravidlá</u>	17. marec 2021

Kontaktujte nás:

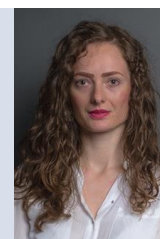
Katarína Ondrovičová
Seniorná advokátka

Tel: +421232332819
katarina.ondrovicova@twobirds.com



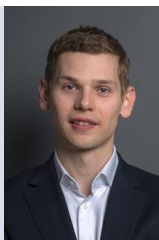
Zuzana Juríčková
Advokátka

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.