sapie | Slovenská aliancia pre inovatívnu ekonomiku

League for Digital Boost

EÚ regulácie ŠPECIÁL

Regulácie digitálnych politík sú jednou z najdôležitejších tém, ktoré sa prerokúvajú nielen na európskej úrovni.

Regulácie do rôznej miery ovplyvňujú veľké, stredné aj malé firmy, mikropodnikateľov, aj samotných spotrebiteľov.

Je preto **dôležité, aby firmy vedeli čo sa ich týka**, ktoré legislatívne návrhy ich ovplyvnia, a v neposlednom rade brať ich názor do úvahy pri zostavovaní legislatívnych rámcov, a zamedziť tak negatívnym nežiaducim dôsledkom.

Autorka: Adriána Tabišová,
Policy Assistant, SAPIE
adriana.tabisova@sapie.sk

Aj preto sme sa rozhodli zaoberať sa regulačnými témami viac, sledovať aktuálne dianie a prinášať Vám novinky z národnej aj európskej úrovne.

Pri tejto príležitosti sme si pre Vás pripravili tento ŠPECIÁL, v ktorom sa dozviete viac o nasledovných návrhoch:

- Akt o digitálnych trhoch (DMA)
- Akt o digitálnych službách (DSA)
- Akt o správe údajov (DGA)
- Akt o údajoch (Data Act)
- Smernica o kybernetickej bezpečnosti NIS1 a NIS2
- Akt o umelej inteligencii (AIA)
- Smernica o kybernetickej bezpečnosti (EU Cybersecurity Act)
- Systém certifikácie kybernetickej bezpečnosti pre cloudové služby (EUCS)

sapie | Slovenská aliancia pre inovatívnu ekonomiku

League for Digital Boost

„Digital is the make-or-break issue.“

Ursula von der Leyen, predsedníčka Európskej komisie, 15. september 2021

Digitalizácii sa na úrovni **Európskej únie (EÚ)** kladie stále viac pozornosti. Momentálna digitálna stratégia EÚ pozostáva z rôznych iniciatív vrátane legislatívnych návrhov v oblasti dát, umelej inteligencie, či kybernetickej bezpečnosti. Cieľom je podporovať digitálne inovácie a zároveň chrániť základné práva občanov EÚ. Navrhovaná legislatíva však **skomplikuje regulačné prostredie pre Vás, podniky** pôsobiace v rôznych online a offline odvetviach.

Preto je potrebné porozumieť a byť informovaný o momentálnych návrhoch. Rozhodli sme sa uľahčiť Vám prácu a zhrnúť základné návrhy, ktoré sú momentálne v hre a **môžu mať dosah aj na Vás.**

Prehľad aktuálnych legislatívnych návrhov a možného vplyvu aj na Vás

Digital Markets Act- DMA (Akt o digitálnych trhoch)

V prípade nedodržiavania Vám hrozia pokuty do výšky 10 % celkového celosvetového ročného obratu Vašej spoločnosti.

DMA posilňuje reguláciu veľkých digitálnych platforiem na úrovni EÚ, ktoré sa označujú ako "gatekeepers". **Nariadenie obsahuje rad odporúčaní a zákazov, ktorých cieľom je zabrániť určitým obchodným praktikám a chrániť menšie podniky.** Povinnosti uložené gatekeeperom majú zabezpečiť lepšiu konkurencieschopnosť a spravodlivosť v digitálnom sektore.

Súčasný stav: Uverejnený v Úradnom vestníku Európskej únie **12.októbra 2022**. DMA nadobudlo účinnosť **1. novembra 2022** a bude sa uplatňovať od **2. mája 2023**.

Medzi kľúčové ustanovenia patria:

- umožnenie interoperability s menšími platformami;
- umožnenie prístupu podnikov k údajom vytvoreným pri používaní platformy gatekeepera;
- obmedzenie kombinácie a krížového používania osobných údajov a používania osobných údajov na cielenú reklamu bez súhlasu;
- zákaz brániť spotrebiteľom v prepojení s podnikmi mimo ich platforiem;
- zákaz brániť používateľom odinštalovať akýkoľvek predinštalovaný softvér alebo aplikáciu.

Ste aj Vy gatekeeperom?

Gatekeeperom ste, ak spĺňate tieto prahové hodnoty:

Príklady zmien, ktoré budete musieť zaviesť, ak ste gatekeeperom:

- zabezpečiť, aby sa koncoví používatelia mohli ľahko odhlásiť zo služieb Vašej platformy alebo odinštalovať predinštalované služby;
- zastaviť predvolené inštalácie softvéru spolu s operačným systémom;
- poskytovať údaje o výkonnosti reklamy a informácií o cenách reklamy;
- umožniť vývojárom používať alternatívne systémy platieb v aplikáciách;
- umožniť koncovým používateľom sťahovať alternatívne obchody s aplikáciami.

V prípade porušovania predpisov Vám hrozí:

- pokuty do výšky 10 % celkového celosvetového ročného obratu Vašej spoločnosti alebo do výšky 20% v prípade opakovaného porušenia;
- pravidelné pokuty do výšky 5 % priemerného denného obratu;
- v prípade systematického porušovania DMA môžu byť po prešetrení trhu uložené ďalšie nápravné opatrenia, kt. budú musieť byť primerané spáchanému priestupku (môžu zahŕňať behaviorálne a štrukturálne nápravné opatrenia, napr. odpredaj časti Vášho podniku).

sapie | Slovenská aliancia pre inovatívnu ekonomiku

League for Digital Boost

Digital Services Act- DSA (Akt o digitálnych službách)

Hrozia Vám pokuty za nedodržanie až do výšky 6 % ročného globálneho obratu spoločnosti.

Cieľom je ochrana digitálneho priestoru pred šírením nezákonného obsahu a zabezpečenie ochrany základných práv používateľov. Kľúčovou myšlienkou je, že **to, čo je nezákonné offline, musí byť nezákonné aj online.** Bude sa vzťahovať na všetkých online sprostredkovateľov, ktorí poskytujú služby v EÚ. **Akt sa zameriava na online sprostredkovateľov, ako sú online trhoviská, cloudové spoločnosti a veľké vyhľadávače.**

Súčasný stav: Uverejnený v Úradnom vestníku Európskej únie **19.októbra 2022**. Začne sa uplatňovať pätnásť mesiacov po nadobudnutí účinnosti.

Medzi kľúčové ustanovenia patria:

- zákaz reklamy určenej maloletým a zákaz používania osobitných kategórií údajov;
- zákaz dark patterns;
- povinnosti týkajúce sa identifikácie a odstraňovania nezákonného obsahu a ďalšie požiadavky na transparentnosť.

Povinnosti sa stupňujú v závislosti od veľkosti a rizika činností; veľké online platformy budú mať dodatočné požiadavky na podávanie správ a audit.

Aký bude mať vplyv na Vás?

- niektoré ustanovenia DSA, ako napríklad zákaz určitej reklamy a dodatočné požiadavky na transparentnosť, znamenajú, že sa budete musieť pozrieť na každé z nariadení GDPR a DSA, aby ste pochopili svoje povinnosti (to isté platí aj pri DMA);
- možné zasahovanie do systému financovania reguláciou reklamy (to by na Vás mohlo mať dosah hlavne, ak ste subjektom kreatívneho priemyslu);
- možný vznik asymetrického dopadu na MSP, pre ktoré môže vyplývať neopodstatnená regulácia obsahu či reklám.

V prípade porušovania predpisov Vám hrozí:

- pokuty za nedodržanie až do výšky 6 % ročného globálneho obratu organizácie;
- za nedodržanie požiadaviek na informácie existujú osobitné sankcie až do výšky 1 % ročného celosvetového obratu;
- pravidelné sankcie v prípade nedodržania rozhodnutí, záväzkov alebo žiadostí o informácie až do výšky 5 % priemerného denného celosvetového obratu.

sapie | Slovenská aliancia pre inovatívnu ekonomiku

League for Digital Boost

Data Governance Act- DGA

Mali by ste preskúmať, či by Vaše činnosti mohli spadať pod služby sprostredkovania údajov.

Cieľom je podporiť zdieľanie a opakované použitie údajov pri súčasnom rešpektovaní ochrany osobných údajov, dôvernosti a práv duševného vlastníctva.

Súčasný stav: Uverejnený v úradnom vestníku **3. júna 2022** s pravidlami, ktoré sa budú uplatňovať od **24. septembra 2023**.

Zahŕňa tri kľúčové oblasti:

- prístup k údajom v držbe orgánov verejného sektora;
- regulácia služieb sprostredkovania údajov;
- podpora "dátového altruizmu" - darovanie údajov pre všeobecné dobro (napr. pre vedecký výskum).

Aký bude mať vplyv na Vás?

- budete môcť profitovať v dôsledku zníženia nákladov na získavanie, integráciu a spracovanie údajov a z nižších prekážok pri vstupe na trhy;
- skráti sa čas potrebný na uvedenie nových produktov a služieb na trh; to umožní MSP vyvíjať nové produkty a služby založené na údajoch.

Hoci sa nariadenie bude vzťahovať predovšetkým na orgány verejného sektora, **mali by ste preskúmať, či by Vaše činnosti mohli spadať pod služby sprostredkovania údajov.** V odôvodneniach DGA sa osobitne spomínajú trhoviská s údajmi a dátové fondy, ktoré môžu byť relevantné najmä v sektore reklamných technológií.

Data Act

Regulácia osobných aj neosobných údajov a väčšia ochrana používateľov.

Cieľom je sprístupňovať viac údajov a stanoviť pravidlá o tom, kto môže aké údaje používať. Zameriava sa na vytvorenie jednotného trhu s údajmi, ktorý umožní ich voľný tok v rámci EÚ a medzi jednotlivými sektormi. **Bude sa vzťahovať na rôzne strany vrátane držiteľov údajov, poskytovateľov cloudových služieb, výrobcov pripojených zariadení a poskytovateľov súvisiacich služieb.**

Týka sa hlavne: **(i) povinného prístupu spotrebiteľov, podnikov a orgánov verejnej služby k údajom ii) zdieľania údajov, ak ide o MSP; a iii) služieb spracovania údajov (prepínanie, medzinárodný prenos neosobných údajov a interoperabilita).**

Súčasný stav: Návrh Európskej komisie uverejnený vo februári 2022. Návrh bol prijatý ITRE výborom v Európskom parlamente vo feburári 2023. **Parlament má o správe rokovať a hlasovať na prvom marcovom plenárnom zasadnutí.**

Medzi kľúčové ustanovenia patria:

- povinnosti "prístupu už od návrhu" (t. j. navrhovanie prepojených produktov a súvisiacich služieb tak, aby používateľom umožňovali jednoduchý prístup a súvisiace práva na prístup, ako aj prenosnosť);
- dodatočné požiadavky na transparentnosť;
- zmluvnú ochranu používateľov a spôsob, akým môže verejný sektor pristupovať k údajom súkromného sektora (v niektorých ohľadoch opak DGA), ale len na účely verejného záujmu;
- nové pravidlá umožňujúce zákazníkom efektívne prepínať medzi rôznymi poskytovateľmi cloudových služieb spracovania údajov;
- spravodlivosť prístupu k údajom a ich používania v obchodných vzťahoch (B2B).

Aký bude mať vplyv na Vás?

- držiteľom údajov ani tretím stranám nebude dovolené ovplyvňovať alebo brániť používateľovi v správaní pri zdieľaní údajov žiadnym nátlakovým, manipulatívnym alebo technickým spôsobom; z týchto prísnych usmernení budete vylúčení, len ak ste mikropodnik, alebo malá spoločnosť nezávislá od iných spoločností;
- Európska digitálna aliancia MSP pripravila pozičný dokument, v ktorom vyzýva tvorcov legislatívy, aby zvážili rozšírenie výnimiek, ktoré sú v súčasnosti určené pre mikropodniky a malé podniky, na všetky MSP;
- najmä poskytovatelia s významným postavením na trhu budú označení ako gatekeeperi; na nich sa budú vzťahovať špecifickejšie obmedzenia, keďže tretie strany nesmú s gatekeepermi zdieľať údaje a gatekeeperi nesmú ani žiadať o prístup k týmto údajom.

NIS1 & NIS2 Directives (Smernica o kybernetickej bezpečnosti)

Členské štáty získavajú právomoc stanoviť sankcie za porušenie NIS2, ako aj pokuty za určité porušenia do výšky 10 miliónov EUR alebo 2 % celkového celosvetového obratu.

Smernica **NIS** o bezpečnosti sietí a informácií bola prijatá v roku 2016 ako prvý právny predpis EÚ v oblasti kybernetickej bezpečnosti. Jej cieľom bolo dosiahnuť **vysokú spoločnú úroveň kybernetickej bezpečnosti v celej EÚ. Právne predpisy sa zameriavajú na zavedenie určitých povinností v oblasti riadenia rizík a podávania**

správ pre prevádzkovateľov základných služieb (napríklad subjekty udržiavajúce kritickú energetickú, zdravotnícku alebo dopravnú infraštruktúru) a poskytovateľov digitálnych služieb (niektorí poskytovatelia online trhov, online vyhľadávačov a služieb cloud computingu).

Súčasný stav: Politickú dohodu formálne prijal Parlament a následne Rada v novembri 2022. Platnosť nadobudla 16. januára 2023 a **členské štáty majú teraz 21 mesiacov, do 17. októbra 2024, na transpozíciu jej opatrení do vnútroštátneho práva. Cieľom NIS2 je nahradiť a posilniť súčasnú smernicu NIS pri riešení nových výziev.**

Kľúčové zmeny vyplývajúce z NIS2:

- NIS2 sa vzťahuje na širší rozsah sektorov a subjektov;
- NIS2 ukladá "riadiacim orgánom" priame povinnosti týkajúce sa implementácie a dohľadu nad dodržiavaním právnych predpisov v ich organizácii - **čo môže viesť k pokutám a dočasnému zákazu vykonávania riadiacich funkcií;**
- NIS2 vyžaduje, aby subjekty zaviedli opatrenia na riadenie kybernetických rizík, ktoré zahŕňajú požiadavky na zmiernenie bezpečnostných rizík a hĺbkovú kontrolu dodávateľov/služieb tretích strán;
- NIS2 ukladá oznamovacie povinnosti vo fázach vrátane **prvotného oznámenia do 24 hodín od zistenia určitých incidentov alebo kybernetických hrozieb** (namiesto jednoduchého "bez zbytočného odkladu" ako v smernici NIS), "priebežných" a "konečných" oznamovacích povinností;

Členským štátom sa udeľuje právomoc stanoviť účinné, primerané a odrádzajúce sankcie za porušenie NIS2, ako aj správne pokuty za určité porušenia do výšky **10 miliónov EUR alebo 2 % celkového celosvetového obratu (podľa toho, ktorá suma je vyššia).**

Artificial Intelligence Act- AIA

Mnoho nových povinností pre podniky využívajúce vysoko rizikové systémy umelej inteligencie (UI).

AIA sa bude vzťahovať na poskytovateľov, používateľov, dovozcov a distribútorov systémov UI. Uplatňuje sa "horizontálne" (vo všetkých odvetviach). Dôraz sa kladie na **bezpečnosť a základné práva občanov EÚ**. Jej cieľom je tiež vytvoriť a upraviť fungovanie rôznych orgánov EÚ a vnútroštátnych orgánov, ktoré budú monitorovať a presadzovať AIA. V AIA sa uplatňuje prístup založený na riziku. Niektoré spôsoby použitia UI sú zakázané, na iné ("vysokorizikové systémy UI" alebo "HRAIS") sa vzťahujú náročné požiadavky a na mnohé sa AIA vôbec nevzťahuje.

Súčasný stav: Parlament má o návrhu zákona hlasovať koncom marca 2023. Po tomto hlasovaní sa v apríli očakáva začiatok diskusií medzi členskými štátmi, Parlamentom a Komisiou (tzv. trialóg). Ak sa tento časový harmonogram dodrží, konečná verzia Aktu by mala byť prijatá do konca roka 2023.

Napriek tomu by ste mali už teraz začať uvažovať o potenciálnom vplyve AIA na Vaše podnikanie. V prípade nedodržania predpisov totiž AIA ukladá značné finančné sankcie.

AIA rozdeľuje umelú inteligenciu do troch kategórií (zakázané, vysoko rizikové a obmedzené riziko). **Väčšina AIA sa vzťahuje na požiadavky vysokorizikových systémov.** Používanie UI spôsobmi, ktoré ovplyvňujú základné práva alebo bezpečnosť používateľov, sa považuje za vysoko rizikové. Patrí sem UI vo vzdelávaní a odbornej príprave, v oblasti zamestnanosti alebo riadenia pracovníkov, základných verejných a súkromných službách (vrátane prístupu k finančným službám), presadzovaní práva, kontrole hraníc a migrácii, či výkone spravodlivosti. UI v týchto odvetviach vytvára širokú škálu právnych povinností pre vývojárov a používateľov.

Prevádzkovatelia vysokorizikových systémov umelej inteligencie musia dodržiavať súlad s predpismi pred a po tom, ako prinesú svoj nástroj UI na trh.

Budete musieť:

- vybudovať systém riadenia kvality;
- udržiavať podrobnú technickú dokumentáciu;
- vykonať posúdenie, aby sa zabezpečila zhoda systému s AIA;
- zaregistrovať systém v databáze EÚ;
- monitorovať systém po jeho uvedení na trh;
- aktualizovať dokumentáciu a posúdenie zhody, ak sa vykonajú podstatné zmeny;
- spolupracovať s orgánmi dohľadu nad trhom.

The EU Cybersecurity Act

Svoje produkty, procesy a služby IKT musíte certifikovať len raz a certifikáty sú uznávané v celej EÚ.

Smernica o kybernetickej bezpečnosti **posilňuje Agentúru EÚ pre kybernetickú bezpečnosť (ENISA) a zavádza rámec certifikácie kybernetickej bezpečnosti produktov a služieb.**

ENISA zohráva kľúčovú úlohu pri vytváraní a udržiavaní európskeho certifikačného rámca pre kybernetickú bezpečnosť tým, že pripravuje technický základ pre konkrétne certifikačné schémy. Má na starosti informovanie verejnosti o certifikačných schémach a vydaných certifikátoch prostredníctvom osobitnej webovej stránky. ENISA má mandát na zvýšenie operačnej spolupráce na úrovni EÚ, pomoc členským štátom EÚ, ktoré ju chcú požiadať o riešenie svojich kybernetických bezpečnostných incidentov, a podporu koordinácie EÚ v prípade rozsiahlych cezhraničných kybernetických útokov a kríz.

Súčasný stav: uverejnená v Úradnom vestníku EÚ 7. júna 2019 a nadobudla účinnosť 27. júna 2019.

Aký bude mať vplyv na Vás?

Cieľom rámca je stanoviť jednotný štandard a zabrániť nejednotnému prístupu, keď jednotlivé členské štáty zavádzajú vlastné normy. **Vy, spoločnosti podnikajúce v EÚ budete benefitovať z toho, že svoje produkty, procesy a služby IKT budete musieť certifikovať len raz a certifikáty budú uznávané v celej EÚ. Zatiaľ sa môžete rozhodnúť, či sa na tomto certifikačnom procese zúčastnite.** Hlavnou výhodou je istota, že zhoda bude uznaná všetkými krajinami Únie.

Certifikácia bude zatiaľ dobrovoľná, pokiaľ nie je v právnych predpisoch konkrétneho štátu EÚ stanovené inak. Očakáva sa však, že sa to v budúcnosti zmení v závislosti od určenej úrovne rizika. Produkty, služby a procesy IKT s nízkou úrovňou rizika by sa mali môcť spoľahnúť na samohodnotenie a/alebo certifikáciu treťou stranou. Očakáva sa, že certifikácia týchto tovarov na "základnej" úrovni zostane dobrovoľná.

EUSC

V roku 2020 agentúra ENISA začala verejnú konzultáciu o novom návrhu systému certifikácie kybernetickej bezpečnosti pre cloudové služby (EUCS) s cieľom zvýšiť dôveru v cloudové služby v celej Európe.

Cieľom schémy je zlepšiť podmienky na vnútornom trhu EÚ s cloudovými službami zefektívnením záruk kybernetickej bezpečnosti služieb. Zámerom návrhu kandidátskej schémy EUCS je harmonizovať bezpečnosť cloudových služieb s predpismi EÚ a medzinárodnými predpismi. **Zo strany niektorých členských štátov a súkromného sektora sa však objavuje silný odpor**, ktorý sa týka najmä požiadaviek na zvrchovanosť v oblasti lokalizácie európskych údajov a zahraničného práva. Požiadavky na suverenitu sa budú ťažko implementovať a kontrolovať, čo povedie k vysokým nákladom a ovplyvní hospodársku súťaž.

V prípade otázok nás neváhajte kontaktovať.

Tím Ligy za digitálny rast a SAPIE.