ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 3:
Zodpovednosť v osobitných oblastiach, Časť. 2

JUDr. Michal Rampášek

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

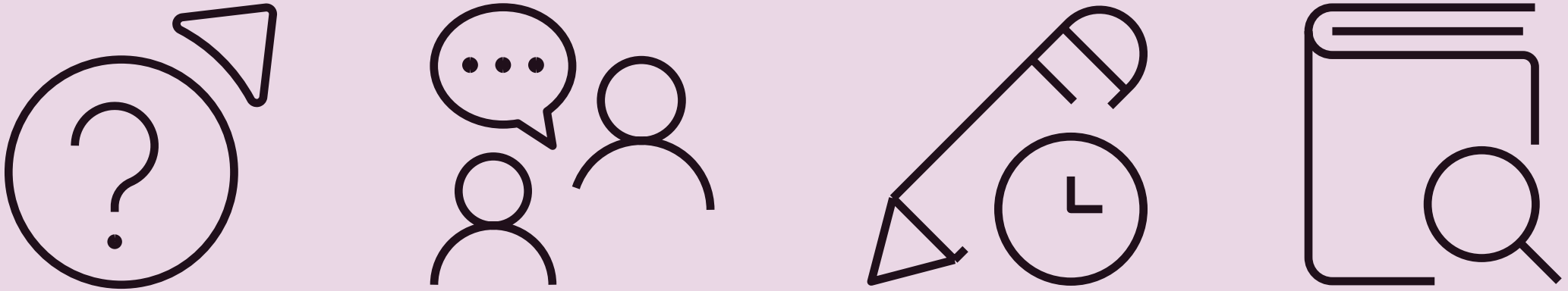
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

- Kybernetická bezpečnosť a GDPR
- Akt o údajoch (Data Act) a Akt o správe údajov (Data Governance Act)
- AI Akt a kybernetická bezpečnosť
- Kybernetická odolnosť finančného sektora (DORA)
- ESG a Kybernetická bezpečnosť

ÚVOD



KYBERNETICKÁ BEZPEČNOSŤ A REGULÁCIA ÚDAJOV

CUSEC

PLÁN OBNOVY

GDPR

Články 32, 33 a 34 GDPR o bezpečnosti osobných údajov

- **GDPR upravuje otázku bezpečnosti osobných údajov a pozostáva z troch samostatných článkov:**
- **článok 32 o bezpečnosti spracúvania** (plus článok 24 povinnosť prevádzkovateľa prijať vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s GDPR),
- **článok 33 o oznamovaní porušenia ochrany osobných údajov dozornému orgánu a**
- **článok 34 o oznamovaní porušenia ochrany osobných údajov dotknutej osobe.**

Článok 32 GDPR Bezpečnosť spracúvania

- Nariadenie EÚ 2016/679
- Prevádzkovateľ a sprostredkovateľ prijmú

i. **so zreteľom** na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako **aj na riziká** pre práva a slobody fyzických osôb,

ii. s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku,

iii. primerané technické a organizačné opatrenia

iv. zahŕňajú aj:

a) pseudonymizáciu a šifrovanie osobných údajov;

b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;

c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;

d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Pri posudzovaní primeranej úrovne bezpečnosti sa **prihliada predovšetkým na riziká ... zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov ... alebo neoprávneného prístupu k takýmto údajom**

Článok 32 GDPR Bezpečnosť spracúvania

- **„vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti zodpovedajúcej riziku“.**
- ako dozorné orgány interpretujú tieto povinnosti v konkrétnych situáciách, napríklad ako chrániť organizácie pred hackerskými útokmi, ako zabezpečiť zmysluplné a robustné šifrovanie alebo ako vytvoriť silné heslá.

Článok 33 GDPR Oznámenie úradu

- **Oznámenie porušenia ochrany osobných údajov dozornému orgánu**
- **V prípade porušenia ochrany osobných údajov, v súlade s povinnosťami stanovenými v článku 33 GDPR, prevádzkovateľ oznámi porušenie príslušnému dozornému orgánu „bez zbytočného odkladu“ a „ak je to možné“, „najneskôr do 72 hodín od zistenia“.**
- V prípade, že oznámenie dôjde po uplynutí 72 hodín, musí obsahovať dôvody omeškania.
- Oznámenie dozornému orgánu sa nevyžaduje, ak je nepravdepodobné, že porušenie ochrany osobných údajov povedie k „riziku pre“ práva a slobody fyzických osôb.
- Prevádzkovateľ zdokumentuje každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

Článok 34 GDPR Oznámenie dotknutej osobe

- **Článok 34 GDPR stanovuje povinnosť prevádzkovateľov údajov oznámiť dotknutým osobám porušenie ochrany osobných údajov „bez zbytočného odkladu“, ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k „vysokému riziku pre práva a slobody fyzických osôb“.**
- Dozorný orgán môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak prevádzkovateľ urobil
- Kedy je potrebné oznámenie dotknutým osobám?
- Prevádzkovateľ prevádzkuje online službu. V dôsledku kybernetického útoku na túto službu sa osobné údaje jednotlivcov stratia.
- Prevádzkovateľ je napadnutý prostredníctvom ransomvéru, čo vedie k zašifrovaniu všetkých údajov. Nie sú dostupné žiadne zálohy a údaje sa nedajú obnoviť. Pri vyšetrovaní sa zistí, že jedinou funkciou ransomvéru bolo zašifrovanie údajov a že v systéme sa nenachádza žiadny iný škodlivý softvér. (Čo však v prípade keby bola k dispozícii záloha a údaje by bolo možné včas obnoviť?)

EDPB

- Európsky výbor pre ochranu údajov
- **Usmernenia 9/2022** týkajúce sa oznamovania porušenia ochrany osobných údajov podľa všeobecného nariadenia o ochrane údajov Verzia 2.0 Prijaté 28. marca 2023
- Porušenie ochrany osobných údajov = „porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.“
- Príkladom straty môže byť situácia, v ktorej jediná kópia súboru osobných údajov bola zašifrovaná prostredníctvom ransomvéru alebo bola zašifrovaná prevádzkovateľom pomocou kľúča, ktorý už prevádzkovateľ nemá k dispozícii.
- Porušenie ochrany osobných údajov je typ bezpečnostného incidentu
- V zásade, zatiaľ čo všetky porušenia ochrany osobných údajov sú bezpečnostnými incidentmi, nie všetky bezpečnostné incidenty sú nevyhnutne porušeniami ochrany osobných údajov

EDPB

- **Bezpečnostný incident,** ktorý vedie k tomu, že osobné údaje sú v určitom období **nedostupné**, je tiež typ porušenia, keďže nedostatočný prístup k údajom môže mať významný vplyv na práva a slobody fyzických osôb.
- Ak sú osobné údaje nedostupné v dôsledku vykonávania plánovanej údržby systému, nepredstavuje „porušenie bezpečnosti"
- Napadnutie prostredníctvom ransomvéru by mohol viesť k dočasnej strate dostupnosti, ak je možné obnoviť údaje zo zálohy. Dochádza však k narušeniu siete a ak sa incident kvalifikuje ako porušenie dôvernosti (t. j. útočník sa dostane k osobným údajom) a to predstavuje riziko pre práva a slobody jednotlivcov, mohlo by sa vyžadovať oznámenie.

EDPB

- Oznámenie uskutočnilo bez zbytočného odkladu, pričom sa **zohľadňuje najmä povaha a závažnosť porušenia, dôsledky tohto porušenia a nepriaznivé dôsledky pre dotknutú osobu**. Týmto sa prevádzkovateľovi ukladá povinnosť zabezpečiť, aby sa včas dozvedel o všetkých porušeniach, aby tak mohol prijať primerané opatrenia. To, kedy presne **možno prevádzkovateľa považovať za „vedomého" konkrétneho porušenia**, bude závisieť od okolností daného porušenia.
- V niektorých prípadoch bude od začiatku pomerne jasné, že došlo k porušeniu, zatiaľ čo v iných prípadoch môže trvať určitý čas, kým sa zistí, či boli osobné údaje ohrozené. Dôraz by sa však mal klásť na rýchle kroky na vyšetrenie incidentu, aby sa zistilo, či bola porušená ochrana osobných údajov a ak áno, na prijatie nápravných opatrení a v prípade potreby na oznámenie.
- Tretia strana informuje prevádzkovateľa, že omylom získala osobné údaje jedného z jeho zákazníkov a poskytne dôkaz o neoprávnenom poskytnutí údajov. Vzhľadom na to, že prevádzkovateľovi sa predložili jasné dôkazy o porušení dôvernosti, nemožno pochybovať o tom, že si je toho „vedomý".
- Prevádzkovateľ zistí, že došlo k možnému narušeniu jeho siete. Prevádzkovateľ skontroluje svoje systémy s cieľom zistiť, či osobné údaje uchovávané v tomto systéme boli ohrozené a potvrdí, že k tomu došlo. Opäť, vzhľadom na to, že teraz má prevádzkovateľovi jasné dôkazy o porušení, nemožno pochybovať o tom, že si je toho „vedomý".

EDPB

- **Vnútorné postupy na odhalenie a riešenie porušenie.**
- Napríklad na nájdenie určitých nezrovnalostí v spracúvaní údajov môže prevádzkovateľ alebo sprostredkovateľ použiť určité **technické opatrenia, ako sú analyzátory toku údajov a logy o aktivite**, z ktorých je možné určiť udalosti a upozornenia korelovaním všetkých údajov z logových súborov. Je dôležité, aby v prípade zistenia porušenia bolo toto porušenie oznámené vyššej príslušnej úrovni riadenia, aby ho bolo možné riešiť a v prípade potreby oznámiť v súlade s článkom 33 a prípadne s článkom 34. Takéto opatrenia a mechanizmy reportingu by mohli byť podrobne opísané v plánoch reakcie na incidenty prevádzkovateľa a/alebo v mechanizmoch riadenia. Tieto pomôžu prevádzkovateľovi účinne plánovať a stanoviť, kto má v rámci organizácie prevádzkovú zodpovednosť za riešenie porušenia a ako alebo či v prípade potreby eskalovať incident.
- Toto krátke obdobie umožňuje **vyšetrovanie a prevádzkovateľ má počas neho možnosť zhromaždiť dôkazy a iné dôležité údaje.** Ak však prevádzkovateľ s primeranou úrovňou istoty zistí, že k porušeniu došlo a ak sú splnené podmienky uvedené v článku 33 ods. 1 GDPR, musí to **bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín** oznámiť dozornému orgánu. Ak prevádzkovateľ nekoná včas a je jasné, že k porušeniu došlo, mohlo by sa to považovať za neoznámenie v súlade s článkom 33 GDPR.

EDPB

- Porušením, ktoré by **NEVYŽADOVALO** oznamovanie dozornému orgánu, by bola strata bezpečne zašifrovaného mobilného zariadenia používaného prevádzkovateľom a jeho zamestnancami. Za predpokladu, že šifrovací kľúč zostane v bezpečnom vlastníctve prevádzkovateľa a nejde o jedinú kópiu osobných údajov, osobné údaje by boli pre útočníka neprístupné. To znamená, že nie je pravdepodobné, že porušenie povedie k riziku pre práva a slobody príslušných dotknutých osôb. Ak sa neskôr ukáže, že šifrovací kľúč bol ohrozený alebo že šifrovací softvér alebo algoritmus je zraniteľný, riziko pre práva a slobody fyzických osôb sa zmení, a preto sa potom môže vyžadovať oznámenie.
- Preto by pri výbere šifrovacieho softvéru prevádzkovatelia mali dôkladne zvážiť kvalitu a správne vykonanie ponúkaného šifrovania, mali by chápať, akú úroveň ochrany skutočne poskytuje a či je to vhodné vzhľadom na uvedené riziká. Prevádzkovatelia by si mali byť vedomí aj špecifík fungovania ich šifrovacieho produktu. Napríklad zariadenie sa môže zašifrovať po vypnutí, ale nie v pohotovostnom režime. Niektoré produkty používajúce šifrovanie majú „predvolené kľúče", ktoré musí každý zákazník zmeniť, ak majú byť účinné. Šifrovanie okrem toho môžu v súčasnosti považovať za primerané, ale o niekoľko rokov môže byť zastarané (post-kvantové šifrovanie), čo znamená, že je otázne, či by boli údaje dostatočne šifrované takýmto produktom a či by sa poskytovala primeraná úroveň ochrany.

Prechod na kvantovo odolnú kryptografiu

Vec C-340/211 , Nacionalna agencija za prichodite

- Rozsudok Súdneho dvora (tretia komora) zo 14. decembra 2023 (vec C-340/211 , Nacionalna agencija za prichodite) ECLI:EU:C:2023:986
- **Prípad sa týka kybernetického útoku na bulharskú Národnú agentúru pre príjmy (NAP), pri ktorom boli zverejnené osobné údaje viac ako 6 miliónov osôb. Fyzická osoba (VB) požadovala náhradu nemajetkovej ujmy z dôvodu obavy, že jej údaje budú zneužité**
- NAP je orgán pridelený bulharskému ministrovi financií. V rámci svojich úloh, ktoré pozostávajú okrem iného z identifikácie, zabezpečovania a vymáhania verejných dlhov, je prevádzkovateľom osobných údajov.
- V tejto súvislosti VB vo veci samej podala žalobu na Administratívny súd Sofia-grad (Správny súd, Sofia, Bulharsko), v ktorej sa domáhala, aby NAP nariadil zaplatiť jej **sumu 1000 leva (BGN) (približne 510 eur) ako náhradu škody na základe článku 82 GDPR** a ustanovení bulharského práva. Na podporu tejto žiadosti uviedla, že utrpela nemajetkovú ujmu v dôsledku porušenia ochrany osobných údajov v zmysle článku 4 ods. 12 GDPR, konkrétnejšie porušenia bezpečnosti spôsobeného nesplnením povinností zo strany NAP vyplývajúcich okrem iného z článku 5 ods. 1 písm. f) a článkov 24 a 32 uvedeného nariadenia. Jej nemajetková ujma spočíva **v obave, že jej osobné údaje, ktoré boli zverejnené bez jej súhlasu, by mohli byť v budúcnosti zneužité, alebo že by sama mohla byť vydieraná, napadnutá alebo dokonca unesená.**

Vec C-340/211 , Nacionalna agencija za prichodite

Závery SDEÚ:

- **Neoprávnené poskytnutie** osobných údajov alebo **neoprávnený prístup** k takýmto údajom „tretími stranami“ samy osebe **nepostačujú na konštatovanie, že technické a organizačné opatrenia prijaté daným prevádzkovateľom neboli „primerané“** v zmysle týchto článkov 24 a 32.
- **Primeranosť technických a organizačných opatrení, ktoré prijal prevádzkovateľ podľa tohto článku, musia konkrétne posúdiť vnútroštátne súdy**, a to s prihliadnutím na riziká spojené s dotknutým spracúvaním a na základe posúdenia, či sú povaha, obsah a vykonávanie týchto opatrení primerané týmto rizikám.
- **Dôkazné bremeno na prevádzkovateľovi**. Ak teda k porušeniu ochrany osobných údajov došlo kybernetickými zločincami, prevádzkovateľ môže byť zbavený zodpovednosti, ak preukáže, že neporušil povinnosti ochrany údajov, ktorým podlieha (C-340/21, body 70 – 72).
- Na účely posúdenia primeranosti bezpečnostných opatrení, ktoré prevádzkovateľ prijal podľa tohto článku, **nemôže znalecký posudok predstavovať systematicky nevyhnutný a dostatočný dôkazný prostriedok**.

Vec C-340/21 a ďalšie

- Prevádzkovateľ sa však **nemôže vyhnúť zodpovednosti odvolávaním sa na nedbanlivosť alebo zlyhanie osoby konajúcej na základe jeho právomoci**, pokiaľ je na prevádzkovateľovi zabezpečiť, aby jeho zamestnanci správne uplatňovali jeho pokyny (rozsudok z 11. apríla 2024, vec C-741/21, juris GmbH, body 49 a 52).
- Okrem toho **existencia nezáväzného poradného stanoviska vydaného prevádzkovateľovi dozorným orgánom nezbavuje prevádzkovateľa zodpovednosti** (rozsudok zo 4. októbra 2024, vec C-200/23, Agentsia po vpisvaniyata, body 174 – 176).

- Vylúčenie limitu de minimis, článok 82 ods. 1 GDPR **vylučuje uplatnenie limitu de minimis pre nemajetkovú ujmu**. To posilňuje právo dotknutých osôb na odškodnenie (C-456/22).
- Dotknuté osoby musia napriek tomu preukázať, že porušenie GDPR spôsobilo nemajetkovú ujmu.
- Nárok na náhradu škody vyžaduje existenciu škody, porušenie GDPR a príčinnú súvislosť.

Vec C-340/211 a náhrada škody

- Zásada zodpovednosti prevádzkovateľa uvedená v článku 5 ods. 2 GDPR a konkretizovaná v jeho článku 24 sa má vykladať v tom zmysle, že v rámci žaloby o náhradu škody založenej na článku 82 tohto nariadenia dotknutý **prevádzkovateľ nesie dôkazné bremeno, pokiaľ ide o preukázanie primeranosti bezpečnostných opatrení**, ktoré prijal na základe článku 32 uvedeného nariadenia.
- **Prevádzkovateľ nemôže byť zbavený svojej povinnosti nahradiť škodu** spôsobenú osobe podľa článku 82 ods. 1 a 2 tohto nariadenia **len preto, že táto škoda vznikla v dôsledku neoprávneného poskytnutia osobných údajov alebo neoprávneného sprístupnenia týchto údajov „tretími stranami“** v zmysle článku 4 bodu 10 uvedeného nariadenia, pričom uvedený **prevádzkovateľ musí preukázať, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu.**
- **Obava z možného zneužitia osobných údajov tretími stranami**, ktorú má dotknutá osoba v dôsledku porušenia tohto nariadenia, **môže sama osebe predstavovať „nemajetkovú ujmu“** v zmysle tohto ustanovenia.

Vec C-687/21, MediaMarktSaturn

- Rozsudok Súdneho dvora (tretia komora) z 25. januára 2024.
- Žalobca vo veci samej navštívil obchodné priestory spoločnosti Saturn, kde si kúpil elektrospotrebič. Na tento účel vyhotovil zamestnanec tohto podniku kúpnu zmluvu a zmluvu o úvere. Pri tejto príležitosti vložil do informačného systému podniku Saturn viacero osobných údajov tohto zákazníka, a to jeho meno a priezvisko, adresu, miesto bydliska, názov zamestnávateľa, jeho príjmy, ako aj bankové údaje.
- Zmluvné dokumenty obsahujúce tieto osobné údaje boli vytlačené a podpísané oboma zmluvnými stranami. Žalobca vo veci samej ich následne odovzdal zamestnancom Saturnu pracujúcim na výdajnom mieste. Iný zákazník, ktorý nenápadne predbehol žalobcu vo veci samej, vtedy omylom prevzal tak spotrebič, ktorý si žalobca objednal, ako aj dotknuté dokumenty a všetko odniesol. Vzhľadom na to, že omyl bol rýchlo zistený, zamestnanec Saturnu dosiahol vrátenie prístroja a dokumentov a ich odovzdanie žalobcovi vo veci samej do polhodiny od ich vydania druhému zákazníkovi.
- Žaloba smerovala k získaniu náhrady nemajetkovej ujmy najmä na základe ustanovení GDPR, ktorú údajne žalobca utrpel z dôvodu pochybenia spôsobeného zamestnancami Saturnu a z toho vyplývajúceho rizika straty kontroly nad svojimi osobnými údajmi.

Vec C-687/21, MediaMarktSaturn

- Rozsudok Súdneho dvora (tretia komora) z 25. januára 2024.
- v rámci žaloby o náhradu škody založenej na článku 82 skutočnosť, že zamestnanci prevádzkovateľa omylom poskytli neoprávnenej tretej strane dokument obsahujúci osobné údaje, **sama osebe nestačí na prijatie záveru, že technické a organizačné opatrenia prijaté dotknutým prevádzkovateľom neboli „primerané" v zmysle týchto článkov 24 a 32.**
- právo na náhradu škody stanovené v tomto ustanovení plní najmä v prípade nemajetkovej ujmy **kompenzačnú a nie sankčnú funkciu** v tom zmysle, že peňažná náhrada založená na tomto ustanovení musí umožniť v plnej miere nahradiť škodu, ktorá konkrétne vznikla z dôvodu porušenia tohto nariadenia.
- osoba žiadajúca náhradu škody na základe tohto ustanovenia **musí preukázať nielen porušenie ustanovení tohto nariadenia, ale aj to, že toto porušenie jej spôsobilo majetkovú alebo nemajetkovú ujmu.**
- v prípade, keď bol dokument obsahujúci osobné údaje poskytnutý neoprávnenej tretej strane, o ktorej je preukázané, že sa s týmito údajmi neoboznámila, „nemajetková ujma" v zmysle tohto ustanovenia nevznikne len na základe samotnej skutočnosti, že dotknutá osoba sa obáva, že v dôsledku tohto poskytnutia, umožňujúceho vykonať kópiu daného dokumentu pred jeho vrátením, dôjde v budúcnosti k šíreniu alebo dokonca zneužitiu jej údajov.

Rozhodnutia národných dozorových orgánov

- **Šifrovanie osobných údajov** bolo stredobodom rôznych rozhodnutí orgánov v oblasti bezpečnosti. V jednom prípade útočník využil bezpečnostnú chybu, ale prevádzkovateľ údajov už mal zavedené šifrovanie HTTPS, dvojfaktorovú autentizáciu a hašovanie hesiel (bcrypt). Orgán nevyhodnotil nedbanlivosť prevádzkovateľa údajov, pretože bezpečnostná chyba sa vyskytla v najnovšej verzii softvéru tretej strany [EDPB:DEBE:OSS:D:2021:211].
- Naopak, v prípade, keď prevádzkovateľ údajov používal **protokol HTTPS** pre svoje webové stránky, ale **nie na stránkach s kontaktnými formulármi**, prostredníctvom ktorých jednotlivci odosielali spoločnosti informácie, ako je meno, e-mailová adresa a akýkoľvek voľný text, orgán zistil, že tento nedostatok šifrovania predstavoval porušenie článku 32 GDPR [EDPB:SE:OSS:D:2021:300].
- V inom prípade bolo **použitie protokolu HTTP namiesto HTTPS** pri prístupe na webovú stránku, vrátane stránky na zber údajov o bankovom účte, považované za nedostatočné bezpečnostné opatrenie, čo viedlo k porušeniu článku 32 GDPR. [EDPB:FR:OSS:D:2023:802].

Rozhodnutia národných dozorových orgánov

- Jeden orgán jasne deklaroval, že **vytvorenie logov udalostí** t. j. zaznamenávanie činností do logových súborov alebo „logov", najmä v prípade prístupu k rôznym serverom informačného systému, je kľúčové, pretože umožňuje sledovať činnosti a odhaľovať akékoľvek anomálie alebo udalosti súvisiace s bezpečnosťou, ako je podvodný prístup a zneužitie osobných údajov. Orgán odkazoval na bezpečnostné odporúčania ANSSI pre architektúru logovacích systémov, ktoré zdôrazňujú dôležitosť a nevyhnutnosť zaznamenávania logov udalostí [EDPB:FR:OSS:D:2021:313].

- Orgány preskúmali zavedenie vhodných **mechanizmov kontroly prístupu**, ktoré je možné zabezpečiť prostredníctvom individuálnej autentifikácie osôb, ktoré majú povolený prístup k špecifickým (súborom) údajov. Absencia takýchto mechanizmov kontroly prístupu viedla k porušeniu článku 32 GDPR [EDPB:FR:OSS:D:2019:73; EDPB:LT:OSS:D:2021:298;

Data Act

Akt o údajoch (DA)

- DA - harmonizované pravidlá o tom, kto môže používať a kto má prístup k strojovo generovaným (osobným a neosobným) údajom v produktoch internetu vecí a súvisiacich službách. GDPR má prednosť.
- Používanie údajov (B2B, B2C)
- Zmluvy týkajúce sa údajov – prispôsobenie postupov a zmlúv týkajúcich sa údajov
- (Návrh) Vzorové zmluvné podmienky (MCT) o prístupe k údajom a ich používaní vrátane podmienok o primeranej kompenzácii a ochrane obchodného tajomstva, ako aj štandardné zmluvné doložky (SCC)
- Presun medzi službami spracúvania údajov (cloud switching) - interoperabilita a prenosnosť údajov
- B2G a žiadosť o výskum

Akt o údajoch a CRA

- Akto údajoch (Nariadenie (EÚ) 2023/2854)
- CRA a Akt o údajoch (DA) majú v podstate odlišnú povahu, pričom prvý stanovuje pravidlá pre sprístupňovanie produktov s digitálnymi prvkami na trhu, zatiaľ čo druhý stanovuje pravidlá pre (okrem iného) sprístupňovanie údajov o produktoch a údajov o súvisiacich službách iným subjektom.
- V určitých prípadoch sa však požiadavky CRA a DA môžu vzťahovať na podobné produkty. V určitých prípadoch môže byť produkt s digitálnymi prvkami v zmysle CRA aj pripojeným produktom alebo súvisiacou službou v zmysle DA.
- Napríklad domáce spotrebiče, ktoré obsahujú hardvér a softvér a ktoré je možné pripojiť k internetu kvôli ich funkčnosti, ako napríklad „inteligentná" chladnička, môžu tiež zhromažďovať údaje o svojom používaní a byť schopné komunikovať tieto údaje o produktoch prostredníctvom Internetu. V tomto zmysle môže byť inteligentná chladnička produktom s digitálnymi prvkami v zmysle zákona CRA a zároveň pripojeným produktom v zmysle DA.
- Ak sa na produkt s digitálnymi prvkami v zmysle CRA môžu vzťahovať aj požiadavky DA na sprístupnenie údajov používateľom alebo tretím stranám (články 4 a 5 DA), výrobca bude musieť zabezpečiť, aby sa v rámci posúdenia rizík zohľadnili aj príslušné požiadavky DA. Výrobcovia by mali mať na pamäti, že hoci DA zaväzuje používateľov a tretie strany poskytovať prístup k údajom o produktoch a súvisiacich službách, zároveň stanovuje opatrenia pre držiteľov údajov, aby v určitých prípadoch obmedzili alebo odmietli zdieľanie údajov (napr. použitím tzv. ručných brzd „obchodného tajomstva" a „bezpečnosti a ochrany" (články 4(8) a 5(11) a 4(2) DA).

Akt o údajoch a GDPR

- GDPR sa plne uplatňuje na všetky činnosti spracovania osobných údajov podľa zákona o ochrane údajov. DA ako taký neupravuje ochranu osobných údajov. DA zlepšuje zdieľanie údajov a umožňuje spravodlivé rozdelenie hodnoty údajov stanovením jasných pravidiel týkajúcich sa prístupu k údajom a ich používania v rámci dátovej ekonomiky EÚ.

- V niektorých prípadoch DA spresňuje a dopĺňa GDPR (napr.: prenosnosť údajov z objektov internetu vecí (IoT) v reálnom čase). V iných prípadoch DA obmedzuje opätovné použitie údajov tretími stranami (napr.: článok 6). V prípade rozporu medzi GDPR a zákonom o ochrane údajov majú prednosť pravidlá GDPR o ochrane osobných údajov (pozri článok 1 (5) DA).

Sprístupnenie údajov

- Iba výrobca efektívne kontroluje prístup a používa vygenerované údaje. Ide o pretvorenie doterajších zmluvných praktík, a to z nárokov na vlastníctvo údajov na povinnosti týkajúce sa správy údajov.
- Údaje generované „pripojeným produktom“ a „súvisiacou službou“ pre používateľa
- Údaje môžu byť sprístupnené „priamo“ (článok 3(1)) alebo „nepriamo“ (článok 4(1)). Možné sú rôzne konfigurácie (napríklad časť údajov by mohla byť sprístupnená priamo a zvyšok by mohol byť sprístupnený nepriamo).
- Priamy prístup znamená, že používateľ má technické prostriedky na prístup, streamovanie alebo sťahovanie predmetných údajov bez toho, aby o to musel požiadať držiteľa údajov. Napríklad pripojený produkt má digitálne rozhranie, kde má používateľ kontrolu nad mechanizmom prístupu, riadi rozhranie a pracovné postupy a kde môže priamo extrahovať údaje z pripojeného produktu.
- Nepriamy prístup znamená, že pripojený produkt alebo súvisiaca služba je navrhnutá tak, že používateľ je povinný požiadať držiteľa údajov o prístup (t. j. proces schvaľovania). Príkladom by bol webový portál, kde môže používateľ podať žiadosť o prístup k údajom.
- Článok 3 DA ponecháva výrobcovi určitú flexibilitu („ak je to relevantné a technicky možné“) v rozhodovaní o tom, či navrhne priamy prístup alebo nie. Je to preto, že nie všetky produkty (a nie všetky údaje) sú navrhnuté tak, aby boli údaje priamo dostupné používateľom.

Rozsah údajov

- Nespracované (raw) a predspracované údaje (jednoducho povedané „nespracované, ale použiteľné“ údaje), ktoré sú držiteľovi údajov ľahko dostupné vďaka technickému návrhu výrobcu, podliehajú povinným povinnostiam zdieľania údajov.
- Údaje, ktoré sa majú sprístupniť, by mali zahŕňať relevantné metaúdaje vrátane ich základného kontextu a časovej pečiatky, aby boli údaje použiteľné, kombinované s inými údajmi, ako sú údaje triedené a klasifikované s inými údajovými bodmi, ktoré sa ich týkajú, alebo preformátované do bežne používaného formátu. Takéto údaje majú potenciálnu hodnotu pre používateľa.
- Naopak, povinnosť držiteľa údajov sprístupniť ich používateľovi alebo príjemcovi údajov, pokiaľ sa údajov nedohodnú inak, sa neuplatní na informácie získané alebo odvodené z takýchto údajov, ktoré sú výsledkom dodatočných investícií do získavania hodnôt alebo poznatkov z údajov, najmä prostredníctvom chránených, komplexných algoritmov vrátane tých, ktoré sú súčasťou proprietárneho softvéru (najmä informácie získané prostredníctvom fúzie senzorov, pri ktorej sa údaje dedukujú alebo sa vyvodzujú z viacerých senzorov a zhromažďujú sa v pripojenom produkte použitím komplexných, proprietárnych algoritmov, a ktoré by mohli byť predmetom práv duševného vlastníctva.)

Pripojené produkty

- Pripojené produkty sú produkty ktoré dokážu generovať, získavať alebo zhromažďovať údaje o svojom používaní, výkone alebo prostredí a ktoré dokážu tieto údaje prenášať prostredníctvom káblového alebo bezdrôtového pripojenia. To zahŕňa aj komunikáciu údajov mimo produktu na ad hoc báze (napr. počas údržby). Pripojené produkty sa nachádzajú vo všetkých oblastiach hospodárstva a spoločnosti. Patria medzi ne inteligentné domáce spotrebiče, spotrebná elektronika, priemyselné stroje, zdravotnícke pomôcky, smartfóny a televízory (recitál 14 DA).

- Produkty, ktoré primárne plnia funkciu ukladania, spracovania alebo prenosu údajov (napr. servery a smerovače), nepatria do rozsahu povinností týkajúcich sa zdieľania údajov podľa kapitoly II DA, pokiaľ ich používateľ nevlastní, neprenajíma alebo nemá v lízingu.

- Podobne skutočnosť, že pripojený produkt (napr. vagón, lietadlo alebo vozidlo) musí na fungovanie používať určitú infraštruktúru (napr. železnice, letiská alebo diaľnice), neoprávňuje používateľa tohto pripojeného produktu na prístup k údajom generovaným napríklad senzormi, ktoré sú súčasťou tejto infraštruktúry. Prístup by bol udelený iba v prípade, že používateľ získal vlastnícke alebo zmluvné práva na senzory zabudované do infraštruktúry.

Súvisiaca služba

- Súvisiaca služba je digitálna služba, ktorú možno prepojiť s prevádzkou pripojeného produktu a ktorá ovplyvňuje funkčnosť tohto pripojeného produktu, napríklad prenosom údajov alebo príkazov doň (napr. aplikácia na nastavenie jasu svetiel alebo na reguláciu teploty chladničky).

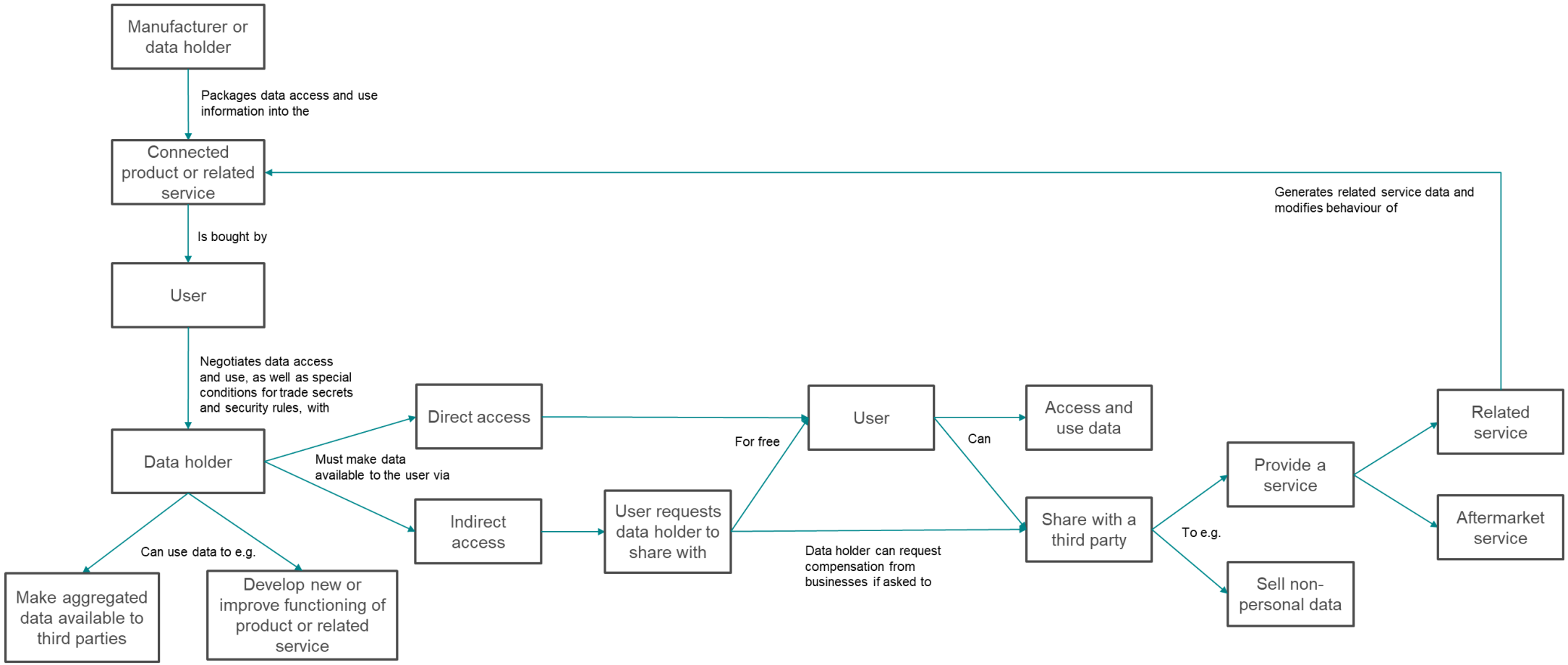
- Na to, aby sa digitálna služba považovala za súvisiacu službu, musia byť splnené dve základné podmienky:

(i) medzi pripojeným produktom a poskytovateľom služby musí existovať obojsmerná výmena údajov, a

(ii) služba musí ovplyvňovať funkcie, správanie alebo prevádzku pripojeného produktu.

Zdroj elektrickej energie ani dodávka pripojenia sa nemajú vykladať ako súvisiace služby podľa tohto nariadenia.

Sprístupnenie údajov



Zdroj: Európska komisia. Prístup k údajom a ich používanie v kontexte internetu vecí

Data Governance Act

Akt o správe údajov (DGA)

- Nariadenie (EÚ) 2022/868: medzisektorový predpis, ktorého cieľom je regulovať **opätovné použitie verejne uchovávaných, chránených údajov posilnením zdieľania údajov prostredníctvom regulácie nových sprostredkovateľov údajov a podporou zdieľania údajov na altruistické účely.** Do rozsahu pôsobnosti zákona DGA patria osobné aj neosobné údaje a všade, kde ide o osobné údaje, sa uplatňuje všeobecné nariadenie o ochrane údajov (GDPR).
- subjektom verejného sektora neukladá žiadna povinnosť umožniť opakované použitie údajov, ani sa ním subjekty verejného sektora nezbavujú svojich povinností zachovávať dôvernosť v súlade s právom Únie alebo vnútroštátnym právom
- Verejné údaje s vysokou hodnotou (napr. geopriestorové, mobilné, environmentálne), ktoré boli predtým nedostupné z dôvodu obáv o súkromie alebo bezpečnosť, sú teraz za určitých podmienok dostupné.
- Smernica 2019/1024 o o otvorených dátach a opakovanom použití informácií verejného sektora upravuje opätovné použitie verejne dostupných informácií, ktoré má verejný sektor v držbe. Verejný sektor však má aj obrovské množstvo chránených údajov (napr. osobné údaje a obchodne dôverné údaje), ktoré nemožno opätovne použiť ako otvorené dáta, ale ktoré by sa mohli opätovne použiť podľa osobitných právnych predpisov EÚ alebo vnútroštátnych právnych predpisov. Z takýchto údajov možno získať množstvo poznatkov bez toho, aby sa ohrozila ich chránená povaha, a zákon o ochrane údajov stanovuje pravidlá a záruky na uľahčenie takéhoto opätovného použitia vždy, keď je to možné podľa iných právnych predpisov.

Akt o správe údajov (DGA)

- Spoločné európske dátové priestory by mali umožňovať, aby údaje boli vyhľadateľné, prístupné, interoperabilné a opakovane použiteľné (ďalej len „zásady správy údajov FAIR“) a zároveň zaistiť vysokú úroveň kybernetickej bezpečnosti.
- Pre výrobcov vytvára príležitosti na zdieľanie, prístup k údajom a ich speňažovanie (vrátane údajov z internetu vecí/zariadení).
- Poskytovatelia sprostredkovateľských služieb údajov (DISP) – registrovaní „neutrálni sprostredkovatelia“ toku údajov od dotknutých osôb a držiteľov údajov k používateľom údajov.
- Spoločnosti musia zabezpečiť bezpečné zdieľanie údajov prostredníctvom akreditovaných sprostredkovateľov, čím sa zabráni neoprávnenému prístupu a únikom údajov.
- Dátový altruizmus (dobrovoľné zdieľanie údajov na základe súhlasu dotknutých osôb so spracúvaním osobných údajov, ktoré sa ich týkajú, alebo povolení držiteľov údajov umožňujúcich použitie ich iných ako osobných údajov na ciele všeobecného záujmu, ako je zdravotná starostlivosť, boj proti zmene klímy, zlepšovanie mobility, uľahčovanie rozvoja, tvorby a šírenia oficiálnych štatistík, zlepšovanie poskytovania verejných služieb, tvorbu verejnej politiky alebo vedecký výskum vo všeobecnom záujme)
- Uznané organizácie pre dátový altruizmus

AI akt

CUSEC

PLÁN OBNOVY

AI Akt

Nariadenie EÚ 2024/1689 ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie

Koho reguluje? Celý ekosystém

Poskytovatelia a výrobcovia výrobkov (väčšina povinností)	Nasadzovatelia („deployers“) (samostatné povinnosti)	Poskytovatelia a nasadzovatelia (splnomocnení zástupcovia poskytovateľov)	Distribútori a dovozcovia (verifikačné povinnosti)	Iná tretia strana	Dotknuté fyzické osoby (súbor práv, najmä právo sťažovať sa, na informácie)
Vyvíja alebo uvádza na trh/do prevádzky systém AI a/alebo GPAI modelu na trh EÚ – bez ohľadu na umiestnenie v EU alebo tretej krajine	Pod koho kontrolou sa systém používa, s výnimkou osobného neprofesionálneho použitia – usadený v EÚ	Usadení v tretej krajine ak výstupy systému AI sú použité v EÚ	Sprístupňujúce/ uvádzajúce na trh systémy AI na trh EÚ	Dodávajúce systém AI, nástroje, služby, komponenty, procesy AI (okrem open-source), ktoré sú integrované do vysokorizikového systému AI	Nachádzajúce sa v EÚ

„**prevádzkovateľ**“
je poskytovateľ, výrobca výrobku, nasadzujúci subjekt, splnomocnený zástupca, dovozca alebo distribútor

Čo reguluje?

Systém AI (čl. 3)

strojový systém, *ktorý je dizajnovaný na prevádzku* ***s rôznymi úrovňami autonómnosti,*** *ktorý môže* ***po nasadení prejavovať adaptabilitu*** *a ktorý* ***pre explicitné alebo implicitné ciele odvodzuje*** *zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie*

- Komisia usmernia k definícii
- Bežný/tradičný softvér je vylúčený
- Zjednotený s OECD definíciou

- Nie je sám o sebe systémom AI
- 2 úrovne: „normálny" GPAI model a GPAI so „systémovými rizikami"

GPAI model (čl. 3)

„model AI na všeobecné účely" je model AI, a to aj model AI trénovaný ***veľkým množstvom údajov*** *s použitím* ***samokontroly vo veľkom rozsahu****, ktorý má* ***významnú všeobecnú povahu*** *a je schopný kompetentne vykonávať* ***širokú škálu odlišných úloh*** *bez ohľadu na spôsob, akým sa model uvádza na trh, a ktorý* ***možno integrovať*** *do rôznych nadväzujúcich systémov alebo aplikácií, s výnimkou modelov AI, ktoré sa využívajú na účely výskumných, vývojových a prototypových činností pred ich uvedením na trh*

https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

Čo (ne)reguluje?

- vymedzením pojmu „systém AI“ by sa mali systémy AI odlišovať od „jednoduchších tradičných softvérových systémov alebo programovacích prístupov, a [toto vymedzenie pojmu by sa nemalo] vzťahovať na systémy, ktoré sú založené na pravidlách vymedzených výlučne fyzickými osobami na automatické vykonávanie operácií.“
- Niektoré systémy majú schopnosť odvodzovať závery úzkym spôsobom, ale napriek tomu nemusia patriť do rozsahu pôsobnosti vymedzenia pojmu „systém AI“, pretože majú obmedzenú schopnosť analyzovať vzorce a autonómne upravovať svoj výstup. Napríklad:
  Systémy na zlepšenie matematickej optimalizácie
- ***Základné spracovanie údajov***
- ***Systémy založené na klasickej heuristike***
- ***Jednoduché predpovedné systémy*** *(použitie priemernej teploty z predchádzajúceho týždňa na predpovedanie teploty na nasledujúci deň. Tento základný systém ochadzuje iba priemerné hodnoty, ale nedosahuje výkonnosť zložitejších systémov predpovedania časových radov, ktoré by si vyžadovali sofistikovanejšie modely.)*

https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

Čo reguluje?

- Podľa AI aktu podliehajú regulačným povinnostiam a dohľadu len určité systémy AI.
- Prístup založený na riziku znamená, že

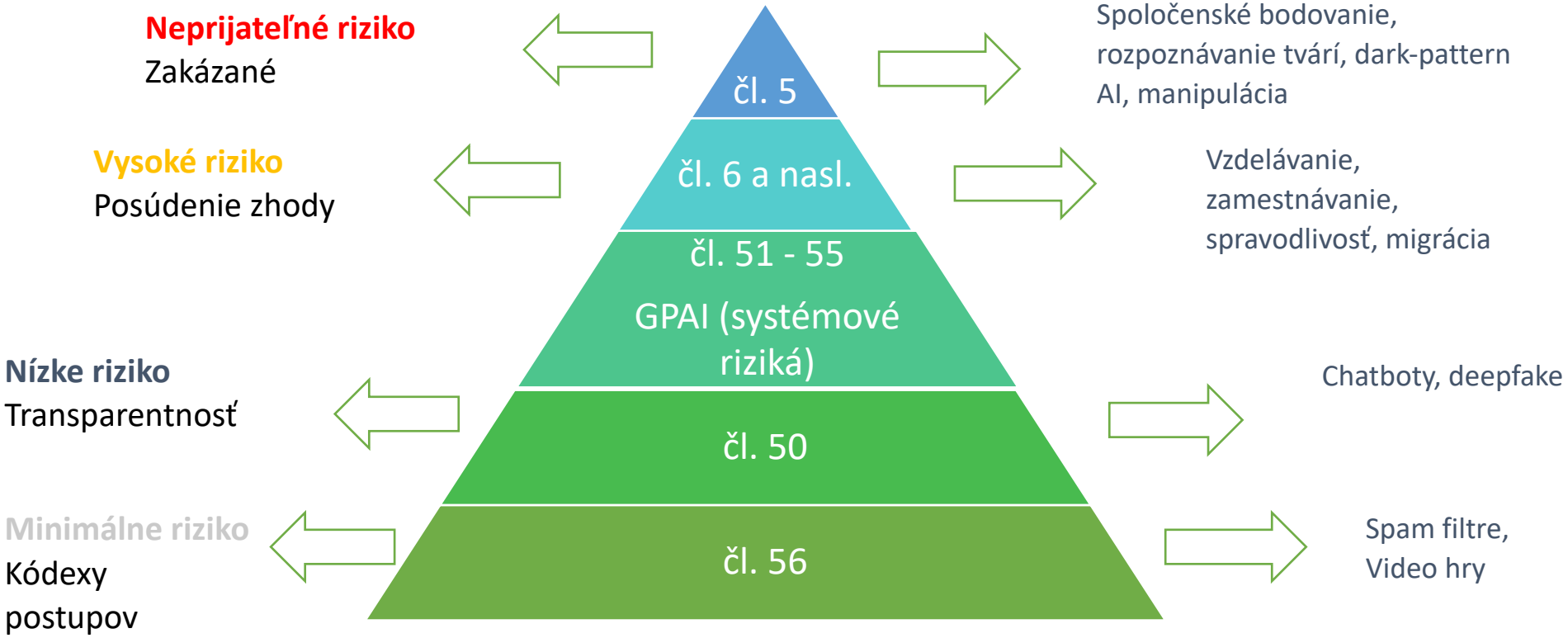
a) zákazy stanovené v článku 5,

b) regulačný režim pre vysokorizikové systémy AI, na ktoré sa vzťahuje článok 6, a

c) požiadavky na transparentnosť pre obmedzený počet vopred vymedzených systémov AI stanovených v článku 50 sa budú vzťahovať len na tie systémy, ktoré predstavujú najzávažnejšie riziká pre základné práva a slobody.

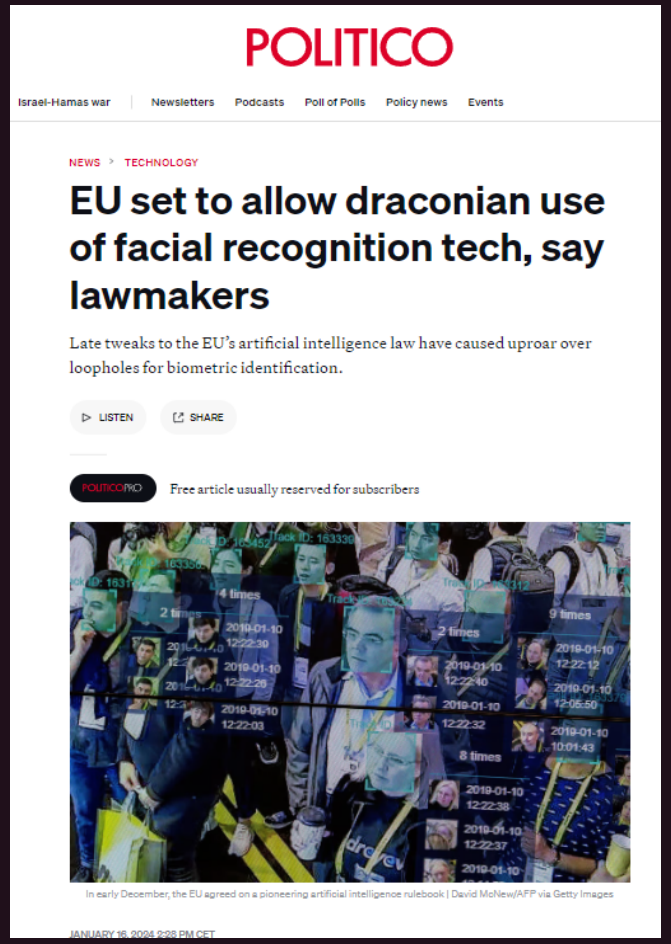
- Prevažná väčšina systémov, aj keď spĺňajú požiadavky na systémy AI v zmysle článku 3 bodu 1, nebude podliehať žiadnym regulačným požiadavkám podľa aktu o AI.

Riziká systémov AI a GPAI



Zakázané praktiky (čl. 5)

- Podprahové techniky (písm.a);
- Manipulácia (písm.b);
- Spoločenské bodovanie (písm.c)
- Individuálne posudzovanie pravdepodobnosti spáchania trestného činu (písm. d);
- Necielené vyhľadávanie (scraping) obrázkov tvárí na internete alebo v kamerových systémoch na účely vytvorenia alebo rozšírenia databáz (písm.e);
- Odvodzovanie emócií fyzickej osoby v oblasti pracoviska a vzdelávacích inštitúcií, pokiaľ to nie je zo zdravotných alebo bezpečnostných dôvodov (písm. f);
- Biometrická kategorizácia fyzických osôb na základe biometrických údajov s cieľom odvodiť alebo vyvodiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie alebo sexuálnu orientáciu (písm.g);
- Diaľková biometrická identifikácia v reálnom čase na verejnosti pri presadzovaní práva, s výnimkami (písm.h).



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Vysokorizikové systémy AI (čl. 6)

- Príloha III - Zoznam 8 oblastí vysokorizikových systémov AI (zmeny cez delegované akty Komisie, len o prípady použitia, nie však oblasti)
- Možnosť poskytovateľa nezaradiť sa = dokumentácia a registrácia systému (čl. 6 ods. 3 a nasl.)

1) Biometria (diaľková biometrická identifikácia, biometrická kategorizácia podľa citlivých charakteristík, **rozpoznávanie emócií**) avšak nie ak jediným účelom je potvrdiť, že konkrétna fyzická osoba je osobou, za ktorú sa vydáva
2) **Kritická infraštruktúra:** systémy AI, ktoré sa majú používať ako bezpečnostné komponenty pri riadení a prevádzke kritickej digitálnej infraštruktúry, cestnej premávky alebo pri dodávkach vody, plynu, tepla alebo elektriny.
3) **Zamestnanosť, riadenie pracovníkov, prístup k SZČO (napr. automatizované filtrovanie CV a hodnotenia uchádzačov)**
4) **Systémy AI, ktoré má používať justičný orgán** alebo ktoré sa majú používať v jeho mene na pomoc justičnému orgánu **pri skúmaní a interpretácii skutkových okolností a práva a pri uplatňovaní práva na konkrétny súbor skutkových okolností alebo ktoré sa majú používať obdobným spôsobom pri alternatívnom riešení sporov**

Povinnosti

Poskytovateľ
vysokorizikových systémov AI
(čl. 16 - 25)

a) Zabezpečovanie súladu systému s požiadavkami čl. 9 - 15
b) Systém riadenia kvality, systém monitorovania po uvedení na trh a oznamovanie závažných incidentov
c) Uchovávanie dokumentácie a logov
d) Posúdenie zhody, Vyhlásenie o zhode, CE
e) Registrácia v databáze EÚ
f) Nápravné opatrenia a informačné povinnosti
g) Preukazovanie zhody systému na odôvodnenú žiadosť orgánu

Nasadzovateľ
vysokorizikových systémov AI
(čl. 26, 27)

a) Vhodné technické a organizačné opatrenia
b) Ľudský dohľad
c) Relevantné a reprezentatívne vstupné údaje
d) Monitorovanie a oznamovacie povinnosti
e) Uchovávanie logov ktoré majú pod kontrolou (max. 6 mes.)
f) Informačné povinnosti voči zamestnancom
g) Informovanie osôb o použití systému AI
h) Posúdenie vplyvu na základné práva (len pre niektoré systémy)

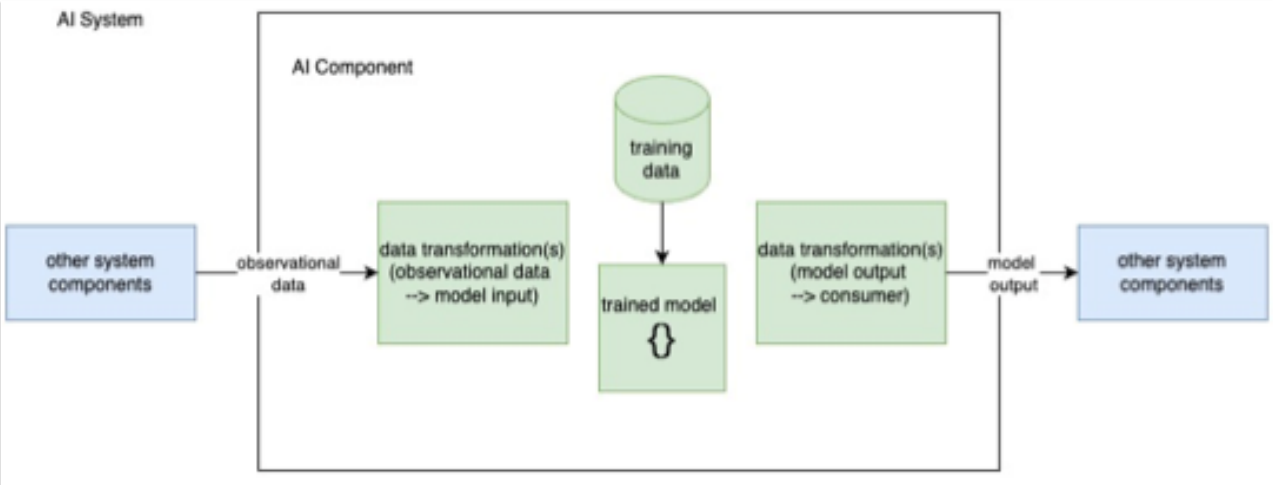
Nízko a minimálne rizikové AI

- **Nízke riziko:**
- Upozorniť osoby, že priamo **komunikujú** so systémom AI, ak to nie je zrejmé z kontextu (napr. chatbotom);
- Zabezpečiť, aby bol **generovaný syntetický obsah** označený v strojovo čitateľnom formáte a zistiteľné **ako umelo vygenerované alebo zmanipulované**;
- Upozorniť na použitie **systému rozpoznávania emócií** alebo **biometrickej kategorizácie**.
- Upozorniť na **generovanie deepfake obsahu a syntetického textu o záležitosti verejného záujmu, okrem redakčnej kontroly**

- **Minimálne riziko:**
- **Každý iný** systém AI
- **Dobrovoľné kódexy**.

Kybernetické riziká AI

Aktíva AI, Algoritmy, Interface, Modely, Údaje, Infraštruktúra
Aké sú aktíva systému AI ?

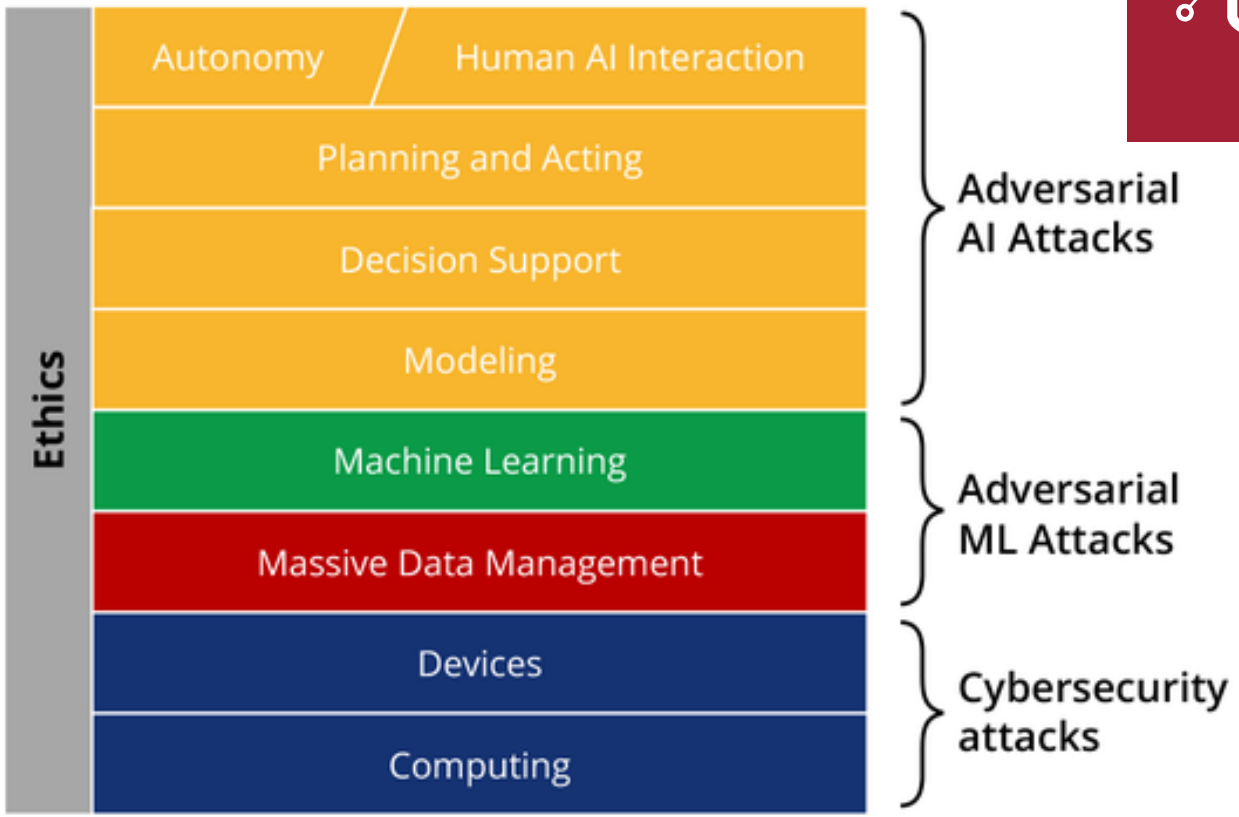


Komponenty systému AI
Householder A.D. et al. 2024

Cyber security risks to artificial intelligence, 15. máj 2024, https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence

Tradičné a nové riziká

MIT AI Risk Repository



CMU/SEI: https://insights.sei.cmu.edu/projects/aisirt-ensures-the-safety-of-ai-systems/

Fáza návrhu

- **Fáza návrhu systémov umelej inteligencie predstavuje kritickú etapu, v ktorej sa kladú základy pre vývoj systému a ktorá zahŕňa rôzne zložité procesy, ako je zber údajov, príprava, plánovanie a návrh modelu.**
- Príklad:
- Zraniteľnosť
- Nedostatok robustnej bezpečnostnej architektúry (AI/softvér) - Odolná bezpečnostná architektúra nie je dostatočne navrhnutá, chýbajú v nej kontroly prístupu, zásady bezpečného návrhu a správne konfigurácie siete
- Zneužitie
- Nedostatok bezpečnostnej architektúry môže umožniť neoprávnený prístup alebo vloženie škodlivého kódu. Vložené poškodené údaje počas trénovania ohrozujú rozhodovanie a skreslujú výstupy.

Fáza vývoja

- **V tejto fáze sa vytvárajú a zdokonaľujú modely umelej inteligencie pre konkrétne úlohy. Táto fáza zahŕňa výber vhodných algoritmov, trénovanie a hodnotenie výkonu modelu. Na zvýšenie presnosti a robustnosti sa vykonávajú iteratívne procesy ladenia a optimalizácie modelu.**
- **Príklad:**
- Zraniteľnosť'
- Nezabezpečené odporúčania kódu umelej inteligencie (AI) – Zraniteľnosti v otvorenom zdrojovom kóde, najmä v nástrojoch ako GitHub Copilot, vyplývajú z obmedzení programovacích modelov. Tieto modely sa môžu neúmyselne naučit' nezabezpečené vzory tvorby zdrojového kódu, čo vedie k odporúčaniam kódu s bezpečnostnými zraniteľnosťami
- Zneužitie
- Využívanie zahŕňa používanie návrhov nezabezpečeného kódu na vytvorenie alebo údržbu softvéru so skrytými zraniteľnosťami. To môže viest' k neoprávnenému prístupu, porušeniu bezpečnosti údajov a šíreniu nezabezpečených postupov tvorby kódu.

Fáza nasadenia

- **Fáza nasadenia označuje prechod vyvinutých modelov AI z vývojových prostredí do reálnych aplikácií. V tejto fáze sa pozornosť presúva na zabezpečenie efektívneho a účinného fungovania riešenia AI v prevádzkových podmienkach. Nasadenie modelu, nastavenie infraštruktúry a monitorovacie mechanizmy sa implementujú na podporu nepretržitej prevádzky systémov AI.**
- Príklad:
- Zraniteľnosť'
- Nezabezpečené koncové body API (AI/softvér) – Zraniteľnosti v rozhraniach, ktoré umožňujú komunikáciu medzi rôznymi komponentmi systému AI, nedostatočné zabezpečenie koncových bodov, ktoré vystavujú funkčnosť' externým subjektom
- Zneužitie
- Využívanie spočíva v tom, že útočníci zneužívajú nedostatočne chránené API na získanie neoprávneného prístupu, zavedenie škodlivých vstupov alebo narušenie bežnej prevádzky systému umelej inteligencie. Dôsledky zahŕňajú neoprávnený prístup k údajom, odmietnutie služby alebo manipuláciu so vstupmi modelu umelej inteligencie.

Fáza údržby

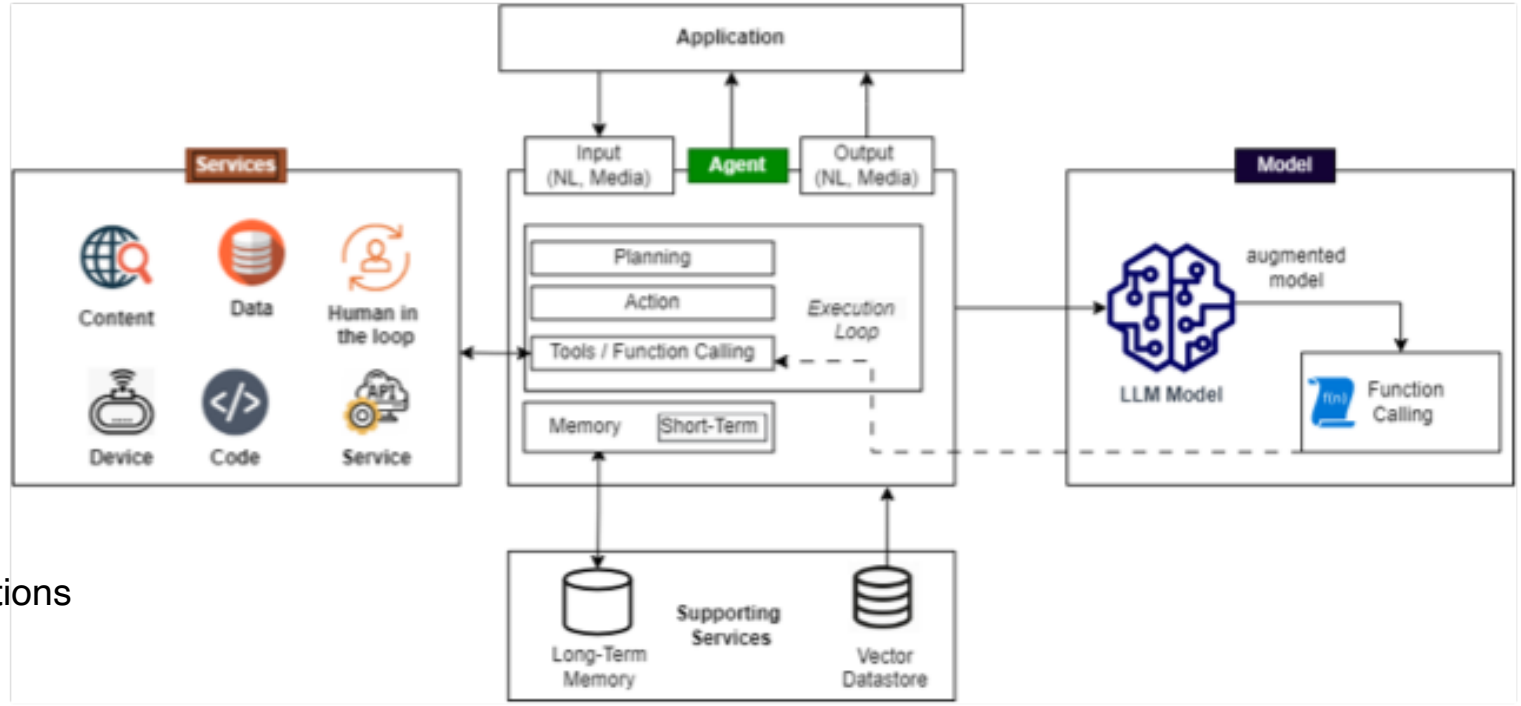
- Vo fáze údržby sa pozornosť presúva na udržanie výkonu a relevantnosti nasadených riešení AI v priebehu času. To zahŕňa priebežné monitorovanie výkonu modelu, kvality údajov a integrity systému s cieľom zabezpečiť pokračujúcu účinnosť v reálnych aplikáciách. Úlohy v tejto fáze zahŕňajú aktualizáciu modelov novými údajmi s cieľom zachovať relevantnosť a presnosť, riešenie akéhokoľvek posunu alebo zhoršenia výkonu a prispôsobenie sa meniacim sa potrebám používateľov alebo zmenám prostredia. Pravidelne sa vykonávajú hodnotenia a audity s cieľom posúdiť výkonnosť riešenia AI na základe vopred definovaných metrík a identifikovať oblasti, ktoré je možné vylepšiť alebo optimalizovať
- Príklad:
- Zraniteľnosť
- Oneskorené bezpečnostné patche (AI/softvér) - Oneskorené bezpečnostné záplaty sa týkajú odloženia aplikovania aktualizácií alebo opráv známych zraniteľností v softvéri a komponentov používaných v AI
- Zneužitie
- Útočníci môžu zneužiť neopravené zraniteľnosti, ohroziť integritu systému, spustiť ľubovoľný kód, manipulovať s modelmi AI alebo získať neoprávnený prístup k citlivým informáciám. Nepriaznivé útoky môžu byť zamerané na známe zraniteľnosti v zastaraných komponentov AI, pokusy o neoprávnený prístup, manipuláciu s modelmi alebo krádež údajov.

Zraniteľnosti

- **Kyberbezpečnosť AI presahuje CIA triádu + kvalita údajov, spoľahlivosť, transparentnosť, vysledovateľnosť**
- Zraniteľnosti AI a strojového učenia sú viacrozmerné – môžu sa prejaviť v údajoch, správaní, výsledkoch alebo interakcii používateľov, nielen v chybách kódu alebo protokolu.
- Bežné alebo očakávané štatistické chyby v modeli AI – napríklad skreslenia alebo nepresnosti vo výstupoch.
- NIS2/ZoKB a CRA vyžadujú riadenie zraniteľnosti, CVD, SBOM, ale chýbajú podrobné usmernenia pre kontexty špecifické pre AI.
- „Zraniteľnosť" je slabá stránka, náchylnosť alebo chyba produktu s digitálnymi prvkami, ktorú môže zneužiť kybernetická hrozba (CRA). Akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou (§ 3 ods. 1 písm. q ZoKB).
- Definícia sa javí ako dostatočne široká na to, aby zahŕňala softvérové komponenty v rámci funkcií založených na ML alebo AI.

Agentická AI – Širšia plocha útoku a nové druhy zraniteľnosti

- Tradičné modely hrozieb umelej inteligencie sa zameriavajú na otravovanie dát, inverziu modelov alebo nepriateľské vstupy.
- Agentická AI ide ďalej s viac komponentovým spracovaním, viacerými agentmi, prompt injection (manipulácia s cieľmi) a poškodením pamäte.
- Architektúra s jedným a viacerými agentmi



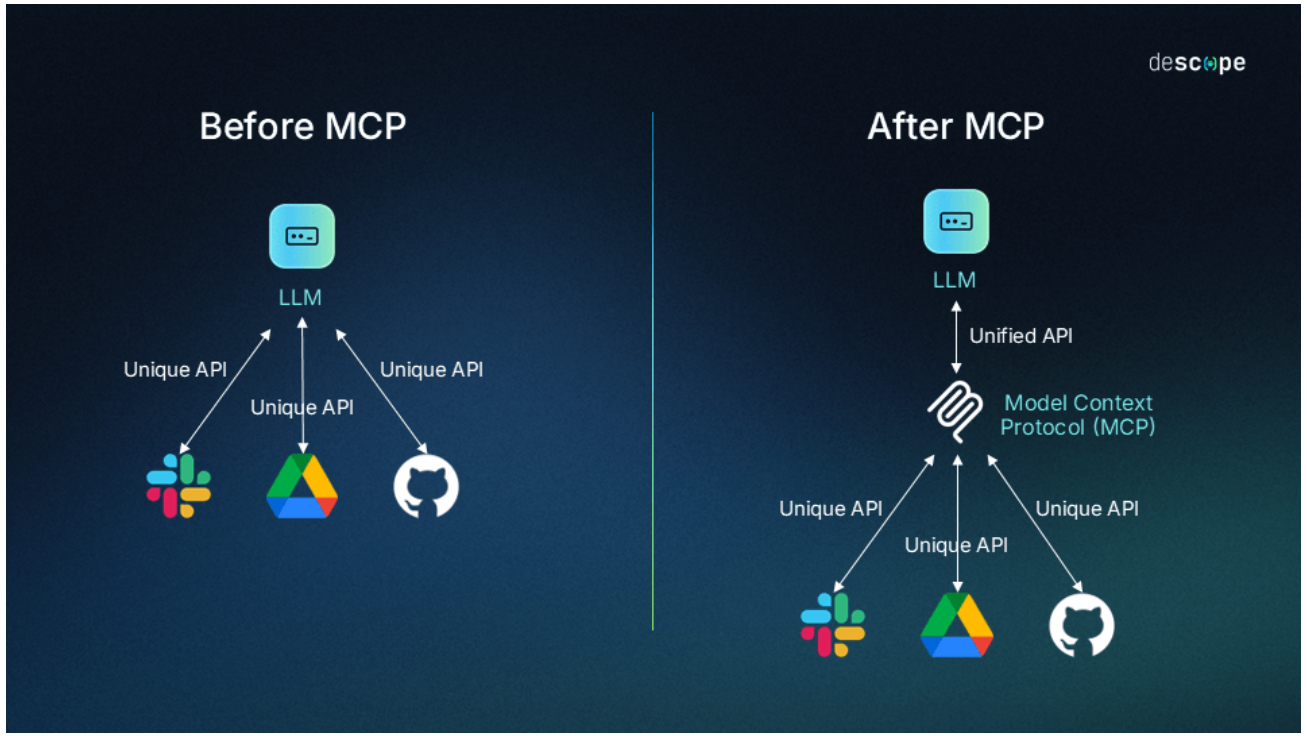
OWASP Agentic AI – Threats and Mitigations
(Feb 2025)

MCP protokol

- Spoločnosť Anthropic vydala ako open-source
- „Most" ktorý umožňuje systémom AI dynamicky interagovať s externými zdrojmi údajov a nástrojmi v reálnom čase.
- MCP nadväzuje na existujúce volanie funkcií tým, že eliminuje potrebu vlastnej integrácie medzi LLM a inými aplikáciami.

Kritická zraniteľnosť v MCP – škodlivý server MCP môže nielen odcudziť citlivé údaje od používateľa, ale aj prevziať kontrolu nad správaním agenta a prepisovať pokyny poskytované inými dôveryhodnými servermi, čo vedie k úplnému ohrozeniu funkčnosti agenta.

Viac: *Narajala V.S., Habler I.:* ***Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies (2025) https://arxiv.org/abs/2504.08623***



Incidenty AI

- „závažný incident“ je **incident alebo porucha** systému AI, ktoré **priamo alebo nepriamo vyústia** do ktorejkoľvek z týchto situácií:

a) **smrť osoby alebo vážna ujma** na zdraví osoby;

b) **vážne a nezvratné narušenie riadenia alebo prevádzky kritickej infraštruktúry (CER a NIS2);**

c) porušenie povinností vyplývajúcich z práva Únie, ktorých cieľom je **ochrana základných práv**;

d) **vážna ujma na majetku alebo životnom prostredí**;

Príklady incidentov AI písm. b)

- Pri hodnotení, či je narušenie nezvratné, je potrebné zohľadnit' nasledujúce aspekty:

a) Porucha si vyžaduje obnovu fyzickej infraštruktúry alebo zničí špecializované zariadenia, ktoré nie sú ľahko dostupné.

b) Kontaminácia vody, pôdy alebo ovzdušia.

c) Strata alebo poškodenie dôležitých záznamov, ako sú údaje o pacientoch, osobné záznamy alebo finančné transakcie, ktoré nie je možné spoľahlivo obnovit' alebo rekonštruovat'.

d) Trvalé vyradenie kritického uzla, ako je železničná križovatka, elektrická rozvodňa alebo pristávacia stanica, ktoré nie je možné opravit' alebo nahradit' bez niekoľkoročnej dodacej lehoty.

e) Strata vesmírneho majetku (napr. globálny navigačný satelitný systém alebo komunikačný satelit), ktorého zničenie uvoľní jeho orbitálnu pozíciu alebo frekvenciu a ktorý nemožno nahradit' bez zdĺhavého postupu výmeny, ktorý zvyčajne trvá roky.

Príklady incidentov AI písm. c)

- Systém náboru založený na umelej inteligencii vylučuje uchádzačov na základe etnickej príslušnosti alebo pohlavia.
- Systém hodnotenia úverovej bonity vylučuje určité kategórie osôb, napríklad osoby s menom pochádzajúcim z určitej oblasti alebo osoby žijúce v určitých štvrtiach.
- Systém biometrickej identifikácie často nesprávne identifikuje osoby s odlišným etnickým pôvodom.

Incidenty AI

- **Poskytovatelia vysokorizikových systémov AI** zavedú systém riadenia kvality, ktorý zahŕňa postupy týkajúce sa oznamovania závažných incidentov (čl. 17)
- Ak **nasadzujúce subjekty** zistia závažný incident, bezodkladne o tom najprv **informujú poskytovateľa** a potom dovozcu alebo distribútora a príslušné orgány dohľadu nad trhom.
- **Poskytovatelia modelov AI na všeobecné účely** so systémovým rizikom sledujú relevantné informácie o závažných incidentoch a možných nápravných opatreniach na ich riešenie, dokumentujú ich a **bez zbytočného odkladu ich oznamujú úradu pre AI a v prípade potreby vnútroštátnym príslušným orgánom**

Rozsiahle porušenie právnych predpisov

- Každé konanie alebo opomenutie v rozpore s právom Únie na ochranu záujmov jednotlivcov, ktoré:

a) spôsobilo alebo pravdepodobne spôsobí ujmu na kolektívnych záujmoch jednotlivcov s pobytom najmenej v dvoch iných členských štátoch, než je členský štát, v ktorom: i) takéto konanie alebo opomenutie malo pôvod alebo sa uskutočnilo; ii) sa nachádza alebo je usadený dotknutý poskytovateľ alebo v relevantnom prípade jeho splnomocnený zástupca, alebo iii) je usadený nasadzujúci subjekt v čase, keď sa tento nasadzujúci subjekt dopúšťa porušenia právnych predpisov;

b) spôsobilo, spôsobuje alebo pravdepodobne spôsobí ujmu na kolektívnych záujmoch jednotlivcov a má spoločné znaky vrátane rovnakého protiprávneho konania alebo porušovania rovnakého záujmu, a ktorého sa dopustil súčasne ten istý prevádzkovateľ v najmenej troch členských štátoch.

Príklady rozsiahleho poškodenia „kolektívneho záujmu jednotlivcov" zahŕňajú: Ochrana životného prostredia, Verejné zdravie, Fungovanie demokratických inštitúcií.

Oznamovanie

Poskytovatelia vysokorizikových systémov AI **hlásia ihneď** po tom, ako poskytovateľ zistí príčinnú súvislosť medzi systémom AI a závažným incidentom alebo logickú pravdepodobnosť takejto súvislosti, najneskôr však **do 15 dní** po tom, ako sa poskytovateľ alebo v relevantnom prípade nasadzujúci subjekt o závažnom incidente dozvedel.

V prípade **rozsiahleho porušenia právnych predpisov alebo závažného incidentu písm. b)** správa sa podá ihneď, najneskôr však **do 2 dní** po tom, ako sa poskytovateľ alebo v relevantnom prípad nasadzujúci subjekt o tomto incidente dozvedel.

V prípade úmrtia osoby správa podá **ihneď** po tom, ako poskytovateľ alebo nasadzujúci subjekt zistí príčinný vzťah, alebo hneď, ako má podozrenie na takýto príčinný vzťah, najneskôr však **do 10 dní**

Môže predložiť prvotnú neúplnú správu, po ktorej nasleduje úplná správa

Bezpečnosť dodávateľského reťazca

- Odkiaľ pochádzajú vaše trénovacie dáta?
- Bol váš LLM testovaný red teamingom?
- Používate multiagentský/agentský proces?
- Ako sa používa/integruje s mojimi dátami?
- Máte dokument o certifikácií SOC2, ISO 27001, ISO27017 (alebo inej bezpečnosti dát)?
- Ako zabezpečujete presnosť výstupov?
- Ako ste skontrolovali/riešili falošné pozitívne výsledky?
- Aký je účel AIvo vašom systéme? Čo robí pre zvýšenie hodnoty?
- Môžem vidieť vaše diagramy/dokumenty procesov/dátových tokov?
- Používate popredný, opensource alebo proprietárny model (LLM)?
- Ponúkate on-prem alebo „air gapped" verziu?
- Aké sú hardvérové/výpočtové požiadavky?

Bezpečnosť dodávateľského reťazca

- Vlastníctvo : Kto vlastní / má práva k modelu? , Kto vlastní dáta? , Kto vlastní výstupy? , Aké sú licenčné požiadavky? (počet volaní, tokeny, cena...)
- Ochrana údajov: Ochrana osobných údajov , Ukladanie a anonymizácia dát , Zmluvy o spracúvaní údajov, Definovanie rozsahu spracovania
- Zodpovednosť: Kto je zodpovedný za chybný výstup AI? Kto je zodpovedný za zneužitie výstupu? (deepfake)
- Etika a regulácia: Dodržiavanie regulačných požiadaviek (AI akt), Zákaz diskriminácie, Testovanie a validácia modelu

Bezpečnosť dodávateľského reťazca

- Transparentnosť a auditovateľnosť: Vysvetliteľnosť, Právo na audit
- Dôvernosť: Ochrana promptov (pred útokom a kto je vlastník volaní), Ochrana algoritmov, Ochrana modelu
- Aktualizácia a údržba modelu: Ako často sa bude model aktualizovať, Kto bude za aktualizáciu zodpovedný, Ako bude vyzerať verziovanie modelov, Právo na starú verziu, ak nová zmení správanie, Rollback mechanizmus
- Kvalita a metriky systému: Presnosť, Recall/Precision, Fairness metriky (bias), Spoľahlivosť
- Audit trail dokumentácia: Ľudský dohľad, konečná zodpovednosť

KYBERNETICKÁ ODOLNOSŤ FINANČNÉHO SEKTORA

Úrovne

Úroveň 1 – Nariadenie

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora

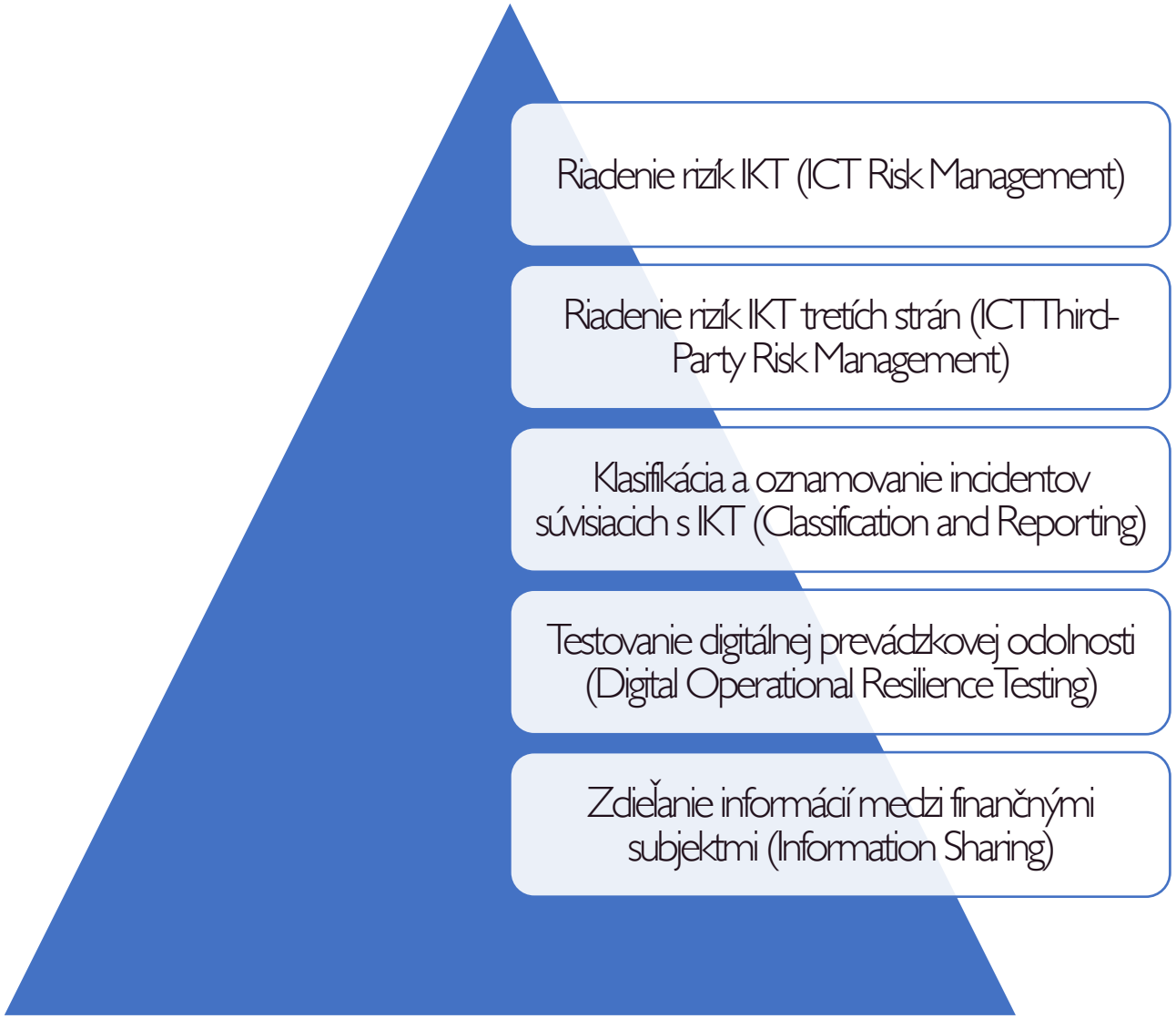
Úroveň 2 – Regulačné, vykonávacie a delegované akty v úradnom vestníku

- RTS o rámci riadenia rizík v oblasti IKT
- RTS o klasifikácii incidentov v oblasti IKT
- RTS o procese hlásenia incidentov v oblasti IKT
- ITS o hlásení incidentov v oblasti IKT
- RTS o penetračnom testovaní na základe hrozieb (TLPT)
- RTS o politike tretích strán v oblasti IKT
- RTS o subdodávkach
- ITS o registri informácií
- DR o kritériách na určenie Critical ICT Third-Party Providers
- DR o poplatkoch za dohľad podľa DORA
- RTS o harmonizácii podmienok dohľadu
- RTS o spoločnom vyšetrovacom tíme (JET)

Úroveň 3 – Usmernenia

- Usmernenia o spolupráci v oblasti dohľadu
- Usmernenia o odhade agregovaných ročných nákladov a strát spôsobených závažnými incidentmi súvisiacimi s IKT

5 pilierov DORA



Riadenie rizík IKT

- Minimalizácia IKT rizík prostredníctvom podrobnejšej identifikácie a ošetrenia rizík
- Riadiaci orgán finančného subjektu nesie konečnú zodpovednosť za riadenie IKT rizík
- Zavedenie komplexného rámca riadenia IKT rizík, ktorý usmerňuje a riadi všetky činnosti súvisiace s IKT rizikami
- Pravidelné testovanie činností reakcie a obnovy (Response & Recovery)

Klasifikácia a oznamovanie incidentov súvisiacich s IKT

- Zavedenie procesu riadenia incidentov súvisiacich s IKT
- Vybudovanie spôsobilostí na monitorovanie, riešenie a následné vyhodnocovanie incidentov
- Klasifikácia incidentov podľa faktorov stanovených v DORA
- Oznamovanie závažných incidentov príslušnému orgánu podľa trojstupňového postupu

Riadenie rizík IKT tretích strán

- Vnímať riziko IKT tretích strán ako integrálnu súčasť rámca riadenia IKT rizík
- Prijať a pravidelne revidovať stratégiu riadenia rizík IKT tretích strán
- Viesť register informácií o všetkých zmluvných vzťahoch s poskytovateľmi IKT služieb tretích strán
- Nastaviť kľúčové zmluvné ustanovenia pre obstarávanie a monitorovanie IKT služieb
- Plniť požiadavky na hodnotenie rizík tretích strán vrátane hodnotení iniciovaných európskymi orgánmi dohľadu (ESA)

- **Zodpovednosť** za súlad je vždy plne zodpovedný finančný subjekt.
- **Proporcionalita** - riadenie rizika musí byť primerané **významu závislostí a kritickosti alebo dôležitosti príslušnej služby**, procesu alebo funkcie, ako aj potenciálnemu **vplyv na kontinuitu a dostupnosť** finančných služieb

Testovanie digitálnej prevádzkovej odolnosti

- Zaviesť primeraný a na riziku založený program testovania digitálnej prevádzkovej odolnosti
- Program na testovanie digitálnej prevádzkovej odolnosti zahŕňa celý rad posúdení, testov, metodík, postupov a nástrojov
- Testovanie nezávislými stranami (nemusia byť externé) s primeranými internými kapacitami na podporu
- Minimálne každoročné testovanie IKT systémov a aplikácií podporujúcich kritické alebo dôležité funkcie
- Povinnosť pre finančné subjekty, ktoré nie sú mikropodnikmi, vykonávať pokročilé „Threat-Led Penetration Testing (TLPT)“ raz za tri roky
- Požiadavky na testovacie subjekty pri vykonávaní TLPT

Zdieľanie informácií medzi finančnými subjektmi

- Vzájomné zdieľanie informácií o kybernetických hrozbách a spravodajských poznatkov (threat intelligence) vrátane ukazovateľov ohrozenia, taktík, techník a postupov, kybernetických bezpečnostných varovaní a konfiguračných nástrojov
- Cieľom výmeny informácií je posilniť digitálnu prevádzkovú odolnosť finančných subjektov
- Prebieha v dôveryhodných komunitách a v súlade s uplatniteľným právom (napr. ochrana údajov, obchodné tajomstvo, hospodárska súťaž)

ESG

ESG (Environmental, Social, and Governance)

- Zodpovedné podnikanie v súlade so zásadami ochrany životného prostredia, sociálnej oblasti a riadenia spoločnosti
- Vykazovanie cieľov a progresu spoločnosti v ESG oblastiach
- Rast hodnoty spoločnosti a jej dôveryhodnosti vo vzťahu k investorom, zamestnancom aj zákazníkom
- Komunikácia firemných hodnôt voči externému prostrediu
- Podpora investícií, ktoré podporujú prechod na udržateľné hospodárstvo

Smernica CSRD

- **Smernica 2022/2464 (CSRD, Corporate Sustainability Reporting Directive)** = požiadavky a povinnosti týkajúce sa vykazovania,
- ESRS štandard = rámec a metodika vykazovania
- Novela zákona č. 431/2002 Z.z. o účtovníctve (§ 20c ods. 11) a zákona č. 423/2015 Z.z. o štatutárnom audite (§ 34a)
- Delegované nariadenie Komisie (EÚ) 2023/2772 z 31. júla 2023, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2013/34/EÚ, pokiaľ ide o štandardy vykazovania informácií o udržateľnosti

- **European Sustainability Reporting Standards (ESRS) S4** (Spotrebitelia a koncových používatelia).

ESRS S4

Tematický ESRS	Aspekty udržateľnosti, na ktoré sa vzťahuje tematický ESRS
SRS S4. Spotrebitelia a koncoví používatelia	Informačné vplyvy na spotrebiteľov a/alebo koncových používateľov, — Súkromie — Sloboda prejavu — Prístup k/ku (kvalitným) informáciám

Správa o udržateľnosti by sa teraz mala zaoberať tým, ako spoločnosť riadi riziká súvisiace s využívaním a zhromažďovaním údajov. Preto musia byť do správy o udržateľnosti zahrnuté opatrenia v oblasti kybernetickej bezpečnosti. Tieto informácie môžu zainteresované strany využiť na posúdenie ochoty podstupovať riziko a potenciálnej dlhodobej ziskovosti spoločnosti. Opatrenia v oblasti kybernetickej bezpečnosti prijaté spoločnosťami musia byť v súlade s povinnosťami v oblasti kybernetickej bezpečnosti stanovenými v právnom rámci EÚ.

Pred prijatím smernice CSRD neexistovali v európskom práve žiadne požiadavky na zverejňovanie informácií týkajúcich sa kybernetickej bezpečnosti. Právny rámec EÚ neobsahoval žiadnu formu ex ante zverejňovania informácií o stave kybernetickej bezpečnosti spoločnosti. V tomto ohľade prinesie smernica CSRD dôležité zmeny.

ESRS S4 Ciele

Podnik môže zdôrazniť osobitné problémy relevantné pre významný vplyv z hľadiska kratšieho obdobia, napríklad iniciatívy týkajúce sa zdravia a bezpečnosti **spotrebiteľov** a/alebo **koncových používateľov** v súvislosti s kontamináciou výrobku alebo so ***závažným porušením súkromia v dôsledku rozsiahleho úniku údajov***.

ESRS S4-4

Požiadavka na zverejňovanie S4-4 – Prijímanie opatrení týkajúcich sa významných vplyvov na spotrebiteľov a koncových používateľov, prístupy k riadeniu významných rizík a využívaniu významných príležitostí súvisiacich so spotrebiteľmi a s koncovými používateľmi a účinnosť týchto opatrení a prístupov

Príklady: Santander banka Poľsko

.. Cieľ je monitorovaný pravidelnými phishingovými testami, ktoré poskytujú praktický vzdelávací prvok pre zamestnancov – tí sa tak naučia techniky používané kyberzločincami... Systém riadenia informačnej bezpečnosti je certifikovaný v súlade s normou ISO/IEC 27001:2013 a zahŕňa dohľad nad informačnou bezpečnosťou v obchodnom prostredí skupiny a posudzovanie špecifických požiadaviek na bezpečnosť informačných a IT systémov.
Adaptčný program, vzdelávanie na intranete, phishingové testy, CyberOctober

V roku 2024 prebiehali súdne a správne konania týkajúce sa našej činnosti v súvislosti s právami zákazníkov.
V súvislosti s ochranou osobných údajov zákazníkov uložil Úrad na ochranu osobných údajov (UODO) banke v roku 2024 finančnú pokutu vo výške 1,44 milióna PLN za neposkytnutie informácií o porušení ochrany údajov v roku 2018.

Postupná implementácia

- Od 1.1.2024 banky, poisťovne, zaisťovne a obchodné spoločnosti – emitenti (viac ako 500 zamestnancov a splnenie aspoň jednej z nasledujúcich 2 podmienok: rok 2022: majetok > 20 mil. EUR, čistý obrat > 40 mil. EUR rok 2023: majetok > 25 mil. EUR, čistý obrat > 50 mil. EUR)
- Od 1.1.2025 všetky veľké ÚJ (veľkostné kritériá podľa účtovnej smernice) (splnenie aspoň dvoch z nasledujúcich 3 podmienok: majetok > 25 mil. EUR, čistý obrat > 50 mil. EUR, počet zamestnancov > 250)
- Od 1.1.2026 kótované malé a stredne veľké ÚJ okrem mikro ÚJ (zjednodušené štandardy)
- Od 1.1.2028 veľké dcérske ÚJ s konečným materským subjektom mimo EÚ

Dopady incidentov na ESG

- Kybernetické riziká môžu viesť k porušeniu súkromia alebo ochrany údajov zákazníkov
- ESRS S4 ukladá vykazovať:

1. **materiálny dopad/riziko (double materiality),** spoločnosti musia posudzovať materiálnosť (významnosť) udržateľnostných tém z dvoch rovnocenných hľadísk, a to impact materiality (dopad na okolie) a financial materiality (dopad na firmu)
2. **governance a procesy (politiky, zodpovednosti, sťažností/nápravy),**
3. **opatrenia a ich účinnosť,**
4. **metriky a ciele (napr. incident rate, školenia, audit, čas nápravy).**