NOVÁ PRÁVNA ÚPRAVA V OCHRANE OSOBNÝCH ÚDAJOV A DOPADY V PRAXI

Demänovská Dolina, 12. októbra 2017

Nariadenie Európskeho parlamentu a rady (EÚ) 2016/679
z 27. apríla 2016
o ochrane fyzických osôb pri spracúvaní osobných údajov
a o voľnom pohybe takýchto údajov,
ktorým sa zrušuje smernica 95/46/ES
(všeobecné nariadenie o ochrane údajov)

uplatňuje sa od 25. mája 2018

POKUTY

do 10 000 000 alebo 2% z celkového svetového ročného obratu

- podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti – 16 rokov
- špecificky navrhnutá a štandardná ochrana osobných údajov (pseudonymizácia, šifrovanie)
- sprostredkovateľ
- - záznamy o spracovateľských činnostiach
- bezpečnosť spracúvania OU
- oznámenie porušenia ochrany OU úradu/dotknutnej osobe
- posúdenie vplyvu
- predchádzajúca konzultácia
- zodpovedná osoba
- mlčanlivosť

do 20 000 000 alebo 4% z celkového svetového ročného obratu

- porušenie niektorej zo zásad vrátane podmienok súhlasu
- nesplnenie alebo porušenie niektorého z práv DO
- povinnosti pri prenose OU

don't panic

Nový zákon o ochrane osobných údajov

(aktuálne v NR SR – číslo parlamentnej tlače 704)

časti nového zákona záväzné pre všetky subjekty upravujú

- vecnú a územnú pôsobnosť zákona
- osobitné situácie spracúvania osobných údajov, ktoré vychádzajú zo splnomocňujúcich ustanovení nariadenia (najmä čl. 9 a kapitola IX, čl. 85 až 91 nariadenia)
- postavenie, pôsobnosť a právomoc úradu
- schvaľovanie kódexov správania prevádzkovateľov a sprostredkovateľov, certifikáciu prevádzkovateľov a sprostredkovateľov, akreditáciu monitorujúcich subjektov a certifikačných subjektov
- vybavovanie sťažností úradom
- kontrolu a konanie o ochrane osobných údajov
- sankcie (správne pokuty a poriadkové pokuty)

Nový zákon o ochrane osobných údajov

(aktuálne v NR SR – číslo parlamentnej tlače 704)

I. časť

- § 5 vymedzenie pojmov – nevzťahuje sa na subjekty, na ktoré sa vzťahuje Nariadenie
- ostatné ustanovenia sa vzťahujú na všetkých prevádzkovateľov

II. časť

- nevzťahuje sa na subjekty, na ktoré sa vzťahuje Nariadenie
- zámer – zachovať konzistentnú úpravu ochrany osobných údajov pre všetkých prevádzkovateľov

III. časť

- pravidlá spracúvania osobných údajov pre prevádzkovateľov, ktorým je príslušný orgán

(prevádzkovateľ informačných systémov Policajného zboru, Vojenskej polície, Zboru väzenskej a justičnej stráže, finančnej správy, prokuratúry, súdov, v ktorých sa spracúvajú osobné údaje na účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchateľov trestných činov, vyšetrovania trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu)

IV. časť

- implementačná/vykonávacia časť zákona
- dopĺňa osobitné pravidlá stanovené Nariadením – osobitné situácie zákonného spracúvania
- na základe splnomocňujúceho ustanovenia
- upravuje spracovateľské operácie (bez súhlasu dotknutej osoby)

V. časť

- postavenie úradu, pôsobnosť, právomoci, personálny aparát
- kódexy správania, certifikácia, akreditácia
- kontrola
- konanie o ochrane osobných údajov
- pokuty, správne delikty, poriadkové pokuty (sankcie)

VI. časť

- spoločné, prechodné a záverečné ustanovenia

Vecná pôsobnosť

Pozitívne vymedzenie

- automatizované, čiastočne automatizované, neautomatizované spracúvanie – ak ide o OU, ktoré tvoria/sú určené na to aby tvorili súčasť IS
- OU na ktoré sa vzťahuje Nariadenie
- OU spracúvané príslušným orgánom (polícia, ZVaJS, FS, prokuratúra, súdy) na účely predchádzania a odhaľovania TČ...trestné konanie

Negatívne vymedzenie

- FO výlučne na domáce alebo osobnej činnosti
- SIS, VS
- NBU na účely vykonávania previerok a na účely zabezpečovania podkladov rozhodovania Súdnej rady SR

Územná pôsobnosť

na spracúvanie OU

- prevádzkovateľom **so sídlom**, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území SR – bez ohľadu na to, kde dochádza k spracúvaniu OU (na/mimo územia SR)

- prevádzkovateľom, ktorý **nemá sídlo**... na území SR, ale na mieste, kde sa na základe medzinárodného práva verejného uplatňuje právny poriadok SR – zahraničné zastupiteľstvá SR

- prevádzkovateľom
  - ✓ ktorý **nemá sídlo**... v členskom štáte
  - ✓ dotknuté osoby sa nachádzajú na území SR
  - ✓ spracúvanie súvisí s ponukou tovaru alebo služieb na území SR (nerozhoduje, či sa vyžaduje od DO platba) alebo
  - ✓ spracúvanie súvisí so sledovaním správania DO na území SR

- voľný pohyb OU medzi SR a členskými štátmi sa zaručuje

ZÁSADY SPRACÚVANIA OU

rešpektovanie základných práv a slobôd DO, aby nedochádzalo k porušovaniu práva na zachovanie ľudskej dôstojnosti, k iným neoprávneným zásahom do práva na ochranu súkromia

Zákonnosť a transparentnosť

- každé spracúvanie má byť zákonné
- potreba disponovať primeraným právnym základom (súhlas, zmluva...)
- právny základ musí byť legálny
- účel spracúvania musí byť legitímny
- informácie musia byť poskytnuté včas, v primeranom rozsahu a zrozumiteľne
- DO má právo vedieť ako sa s jej OU nakladá, ako sú spracúvané, správať sa v medziach rozumného očakávania DO (informačná povinnosť)

Obmedzenie účelu

- účel – jasný, zrozumiteľný
- musí byť z neho zrejmé aké sú očakávané spracovateľské operácie, zoznam/rozsah OU, lehota uchovávania – povinnosť informovať DO
- nesmú sa ďalej spracúvať spôsobom nezlučiteľným s pôvodným účelom
- zlučiteľnosť účelov – netýka sa privilegovaných účelov (archivácia, veda, história, štatistika)

Minimalizácia OU

- v nevyhnutnom rozsahu vo vzťahu k účelu
- vždy zvážiť každú spracovateľskú operáciu – jej nevyhnutnosť

Správnosť OU

- správne, aktuálne, opatrenia na vymazanie alebo opravu nesprávnych

Minimalizácia uchovávania OU

- uchovávanie vo forme, ktorá umožňuje identifikáciu DO, kým je to potrebné na účely
- dlhšie – výlučne na privilegované účely – ak sú dodržané primerané záruky ochrany práv a slobôd

Integrita a dôvernosť

- ochrana pred náhodnou stratou, zničením, poškodením – bezpečnostné opatrenia

Zodpovednosť prevádzkovateľa

- dodržiavanie zásad, súlad so zásadami
- preukazovanie súladu

Zodpovednosť prevádzkovateľa

- prijať vhodné technické a organizačné opatrenia (povaha, rozsah, kontext, účel, riziká pre práva a slobody FO)
- zabezpečiť a preukázať súlad
- **živé** - podľa potreby preskúmať a aktualizovať
- zavedenie politík ochrany údajov
- preukázanie splnenia povinností – napr. dodržiavanie schválených kódexov, certifikačných mechanizmov

odporúčanie – splnenie povinností dokumentovať - preukazovanie

Základné zmeny

maloletý

- služby informačnej povinnosti (právny základ súhlas)
- 16 rokov

fotografia

- osobitná kategória - nie

oznamovacia a registračná povinnosť

- vedenie záznamov o spracovateľských činnostiach

priamy marketing

- oprávnené záujmy prevádzkovateľa (primerané očakávanie)

spracúvanie už zverejnených osobných údajov

- in relevantný právny základ – súhlas dotknutej osoby, oprávnený záujem

priamy marketing v poštovom styku, jednorazový vstup do budovy, monitorovanie priestoru prístupného verejnosti

- ako právny základ zaniká

vnútroštátna právna úprava

bez súhlasu DO

- účel akademický, umelecký, literárny (zachovanie práv DO)
- informovanie verejnosti masovokomunikačnými prostriedkami – v predmete činnosti
- zverejnenie, poskytnutie na pracovné účely
- osobitná úprava pre **rodné číslo – nie je osobitnou** kategóriou
- ochrana práv FO, ktorá poskytuje OU o inej FO

bezpečnosť – medzinárodné normy a štandardy

OU o zosnulej osobe

- zákon sa vzťahuje (úprava oproti Nariadeniu)

ZODPOVEDNÁ OSOBA

- **nie je osobne zodpovedná za nesúlad** s GDPR
- ak P/S poverí dobrovoľne, vzťahujú sa rovnaké pravidlá podľa N/Z
- ak P/S nie je si istý – interná analýza, či má povinnosť poveriť ZO (zodpovednosť prevádzkovateľa)

- prípady **obligatórneho** určenia
  - ✓ orgán verejnej moci / verejnoprávny subjekt (s výnimkou súdov pri výkone ich súdnej moci)
  - ✓ Hlavná činnosť P/S
    - pravidelné a systematické monitorovanie DO vo veľkom rozsahu
    - spracúvanie osobitných kategórií OU vo veľkom rozsahu / údajov týkajúcich sa uznania viny za TČ a priestupky
  - ✓ príslušný orgán (predchádzanie a odhaľovanie TČ)

hlavná činnosť

- spracúvanie je nevyhnutné na to, aby P/S dosiahol svoj zamýšľaný cieľ – hlavné činnosti
- pracúvanie OU je neoddeliteľnou súčasťou hlavnej činnosti
- napr. nemocnica, SBS, sprostredkovateľ – personálna agenda (veľa malých firiem)

vo veľkom rozsahu

- značný objem OU na regionálnej, vnútroštátnej alebo nadnárodnej úrovni
- môže ovplyvniť veľký počet DO
- pravdepodobne spracovanie povedie k vysokému riziku
- napr. nemocnica, MHD, banka, poisťovňa,
- **spracovanie údajov (obsahu, prevádzkových a lokalizačných údajov) poskytovateľmi telefónnych a internetových služieb**

pravidelné a systematické monitorovanie

- všetky formy sledovania a profilovania na internete (analýza správania, zisťovanie osobných preferencií)

kto?

- právnická osoba – podmienky (určenie osoby v zmluve)
- fyzická osoba
- zamestnanec
- odborné znalosti

Stanovisko WP29

- Zodpovedné osoby by mali mať expertíznu znalosť národného ako aj európskeho práva na ochranu osobných údajov ako aj hĺbkovú znalosť GDPR;
- Zodpovedná osoba by tiež mala mať dostatočnú znalosť vykonávaných spracovateľských operácií, informačných systémov a bezpečnosti dát.

Prevádzkovateľ vz. sprostredkovateľ

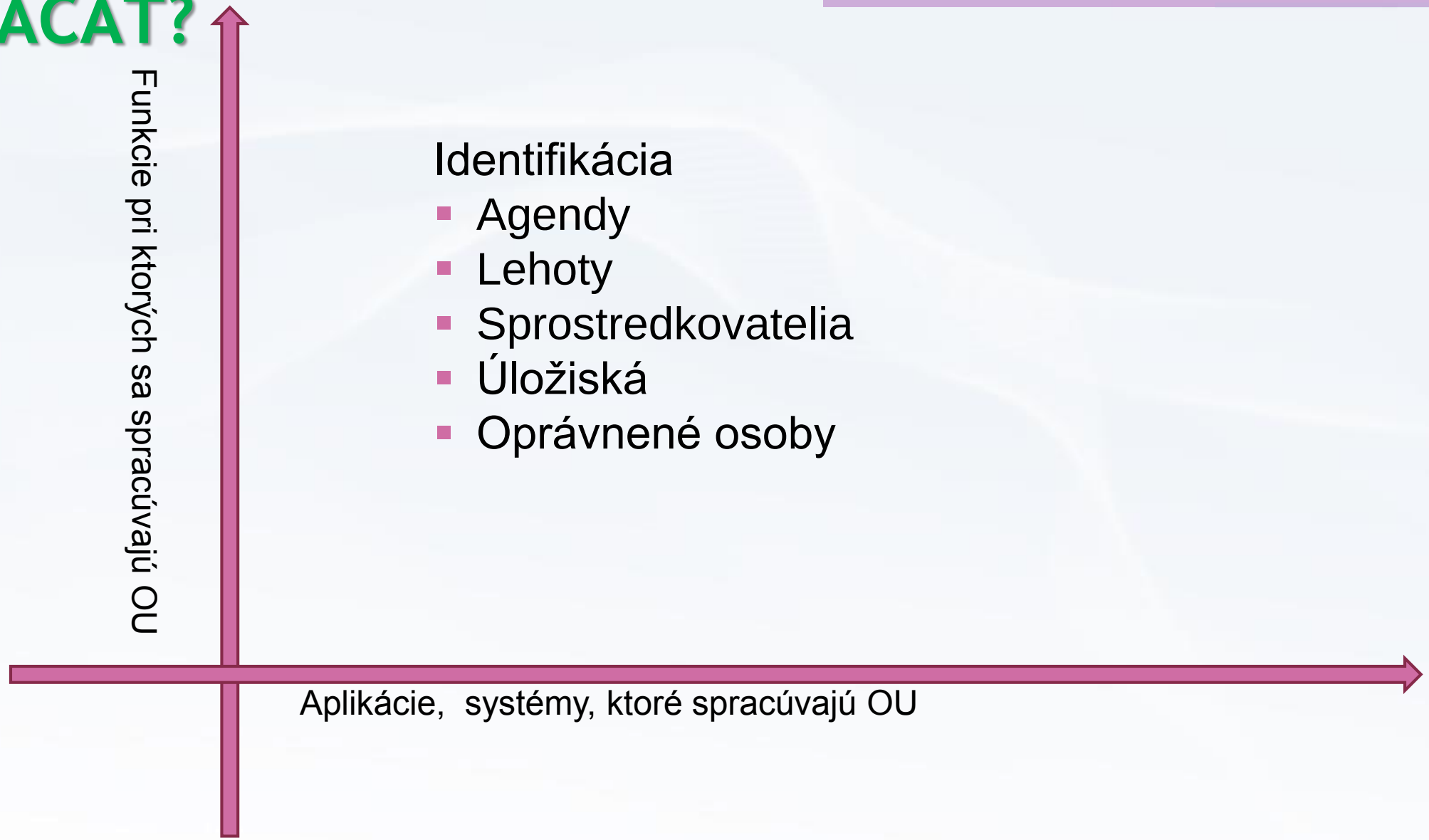
povinnosti prevádzkovateľa/sprostredkovateľa

- zabezpečiť priamu reportovaciu „linku“ na vedenie spoločnosti
- podporovať v plnení úloh
- zverejniť kontaktné údaje (nemusia to byť OU)
- oznámiť kontaktné údaje dozornému orgánu
- umožniť nezávislú činnosť
- posúdenie vplyvu
- porušenie ochrany OU – B incident
- nesúlad názorov – dokumentovať prečo sa neakceptovali návrhy a postupy ZO
- nemôže byť postihovaná pre výkon svojich povinností

povinnosti ZO

- poskytovanie informácií a poradenstva P/S v oblasti ochrany OÚ
- monitorovanie súladu, zvyšovanie povedomia, odborná príprava personálu
- poradenstvo k posúdeniu vplyvu na ochranu údajov a monitorovanie jeho vykonávania
- spolupráca s dozorným orgánom
- kontaktné miesto pre DO, pre dozorné orgány ako aj odborné poradenstvo pre P/S
- aj iné úlohy, ak tam nie je konflikt záujmov

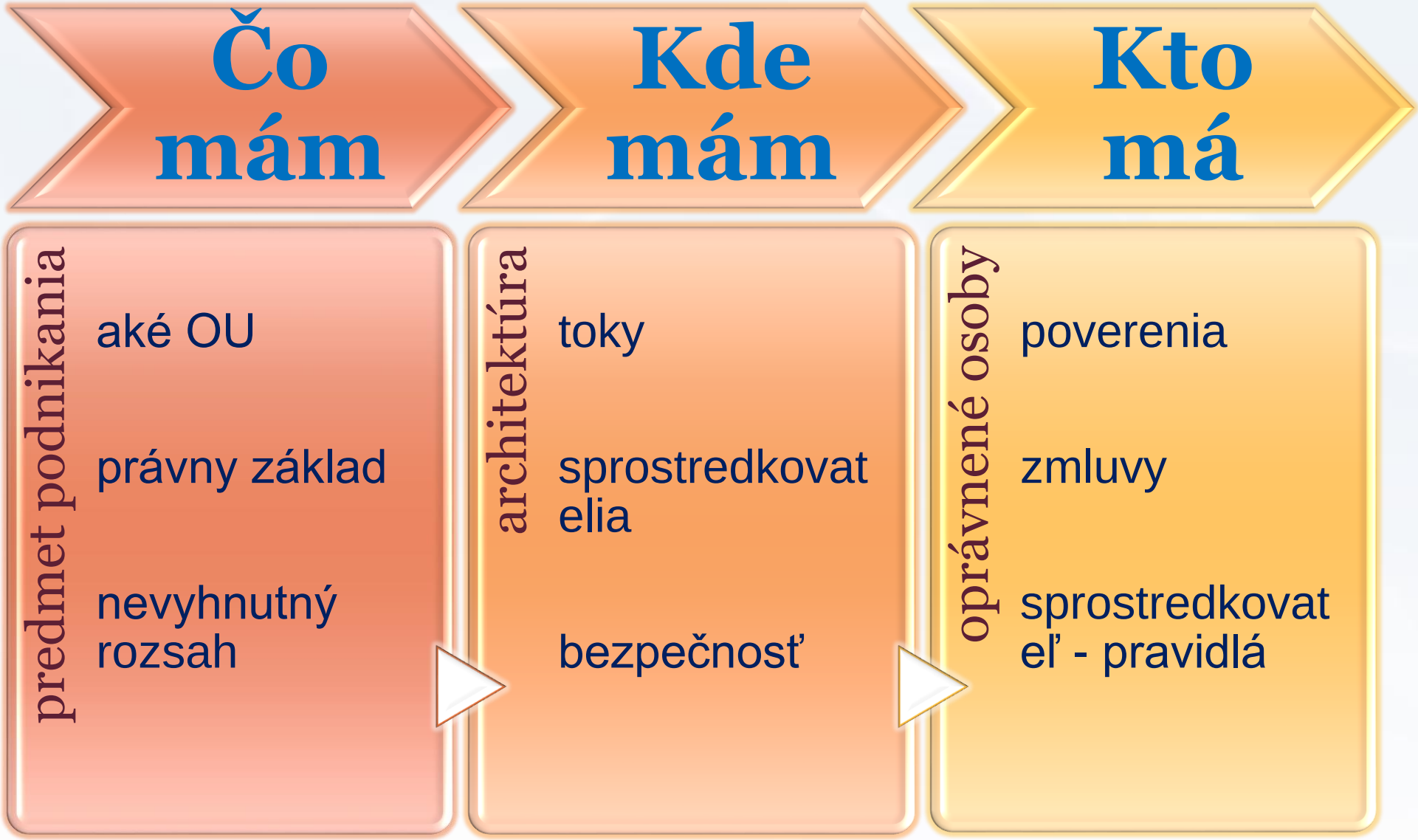
AKO ZAČAŤ?



Identifikácia

- Agendy
- Lehoty
- Sprostredkovatelia
- Úložiská
- Oprávnené osoby

ZMAPOVANIE PROSTREDIA



PROJEKTOVÝ PLÁN

Mapovacia fáza (dáta – procesy)

Analýzy

Vyhodnotenia

Nové procesy a zabezpečenia

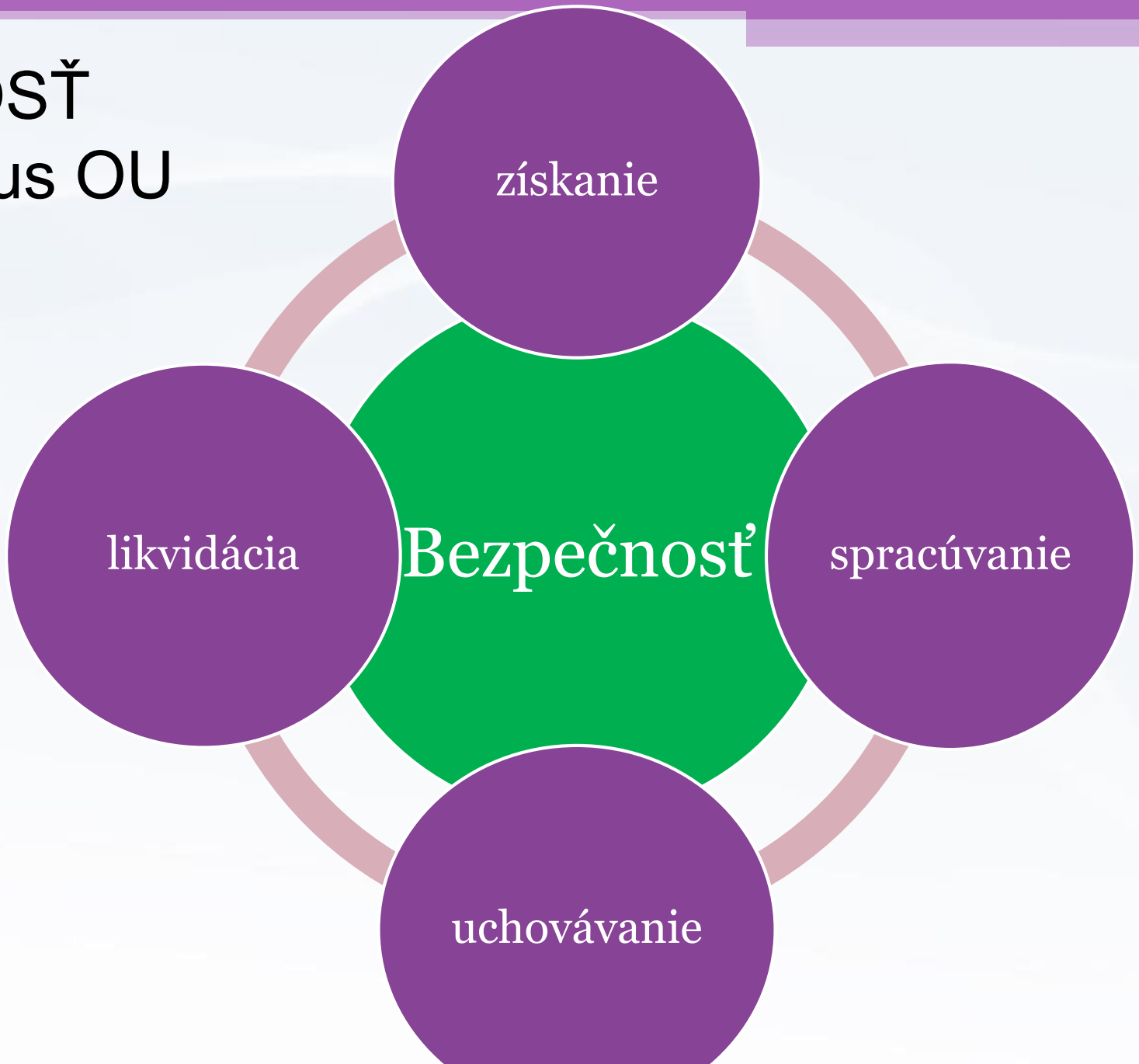
Preverenie vzťahov

Implementácia bezpečnostných opatrení

BEZPEČNOSŤ

- každý prevádzkovateľ je povinný prijať primerané bezpečnostné opatrenia
- povinnosť prevádzkovateľa
- musí zodpovedať podmienkam spracúvania
- musí zohľadniť riziká – ich pravdepodobnosť a závažnosť pre práva a slobody FO
- opatrenia musia byť primerané riziku
- na ich identifikáciu a zhodnotenie rizík musí prevádzkovateľ identifikovať všetky spracovateľské operácie
- vedieť popísať celý životný cyklus osobných údajov od momentu ich získania až po likvidáciu

BEZPEČNOSŤ
Životný cyklus OU



- kontrola na spracovateľskými operáciami
- kto
- čo
- ako
- kedy
- podmienky

CIEĽ

bezpečnosť – eliminácia možných rizík a dopadov

POVINNOSŤ

vždy prijať primerané bezpečnostné opatrenia – **preukázať ich prijatie** (zásada zodpovednosti)

Bezpečné spracúvanie – základné opatrenia

- dôvernosť
  len ten komu sú určené
- integrita
  nepozorovaná modifikácia
- dostupnosť
  prístup k údajom
- odolnosť systémov a služieb
- schopnosť obnoviť – incident
  zálohovanie
- testovanie, posudzovanie, hodnotenie BP – pravidelne
- šifrovanie (silná šifra), pseudonymizácia
- kódex správania, certifikát
- každá FO, konajúca za prevádzkovateľa/sprostredkovateľa, ktorá má prístup k OU – spracúva ich podľa pokynov **prevádzkovateľa**

pseudonymizácia

- stále sú to OU – identifikovateľná osoba
- oddelené uchovávanie OU bez možnosti priradiť k DO, bez dodatočnej informácie

!!!

- jej zavedenie nevylučuje aplikáciu ďalších opatrení
- jeden z mechanizmov, nie však jediný
- nezaručuje automaticky bezpečné spracúvanie
- vždy spolu s ďalšími zavedenými a aplikovanými mechanizmami
- nemám istotu = posúdenie vplyvu = zostatkové vysoké riziko = predbežná konzultácia
- návrh na možné lepšie riešenie a ošetrenie rizika, príp. akceptácia
- nemusí byť vždy riešením

Prevádzkovateľ

medzinárodné normy a štand.

VŽDY
prijať BO

zachová aj Zákon/ Nariadenia

technické
personálne
organizačné

posúdenie vplyvu

bez posúdenia vplyvu

Posúdenie vplyvu – KEDY?

- spracúvanie prostredníctvom nových technológií
- s ohľadom na podmienky spracúvania povedie k vysokému riziku pre práva a slobody FO
- posúdenie plánovaných spracovateľských operácií
- pred začatím spracúvania

Vždy povedie k vysokému riziku

- systematické a rozsiahle hodnotenie osobných aspektov FO vrátane profilovania (autom. rozhodovanie s právnym účinkom)
- spracúvanie OU vo veľkom rozsahu - osobitná kategória, biometria, uznanie viny (posúdenie rozsahu v kontexte podmienok spracúvania)
- systematické monitorovanie verejne prístupných miest vo veľkom rozsahu
- ďalšie spracovateľské operácie úrad vydá vo vykonávacom predpise

Posúdenie vplyvu

- **posudzujú sa hrozby, zraniteľnosti, dopady a riziká vo vzťahu k ohrozeniu práv fyzickej osoby** (NIE dopad na prevádzkovateľa)
- zmapovanie životného cyklu OU, podmienky spracúvania, účel,
- primeranosť vo vzťahu k účelu
- zdroj, povaha, osobitosť, vážnosť rizika pre práva a slobody DO
- posúdenie technických, personálnych, organizačných opatrení
- audit ochrany osobných údajov, kontrola zodpovednou osobou...

Predchádzajúca konzultácia

- posúdil vplyv, identifikoval vysoké riziko, prijal opatrenia na zmiernenie rizika
- zvyškové riziko – ostalo vysoké aj napriek prijatím opatreniam na jeho zmiernenie

Bezpečnostný incident

oznámenie úradu do 72 hodín

- ide o porušenie ochrany OU a zároveň
- musí viesť k riziku pre práva a slobody FO
- a prevádzkovateľ sa o ňom dozvedel

- prevádzkovateľ musí mať prijaté mechanizmy na zhodnotenie každého bezpečnostného incidentu tak, aby bol schopný identifikovať, či ide o porušenie ochrany OU a či to viedlo alebo môže viesť k riziku pre FO

- lehota na nahlásenie začína plynúť momentom, kedy prevádzkovateľ zhodnotil

- spoločné nahlasovanie prostredníctvom JISKB (nie je povinné pre všetkých, upraví zákon o kybernetickej bezpečnosti)

Ďakujem za pozornosť

Tatiana Valentová
tatiana.valentova@pdp.gov.sk