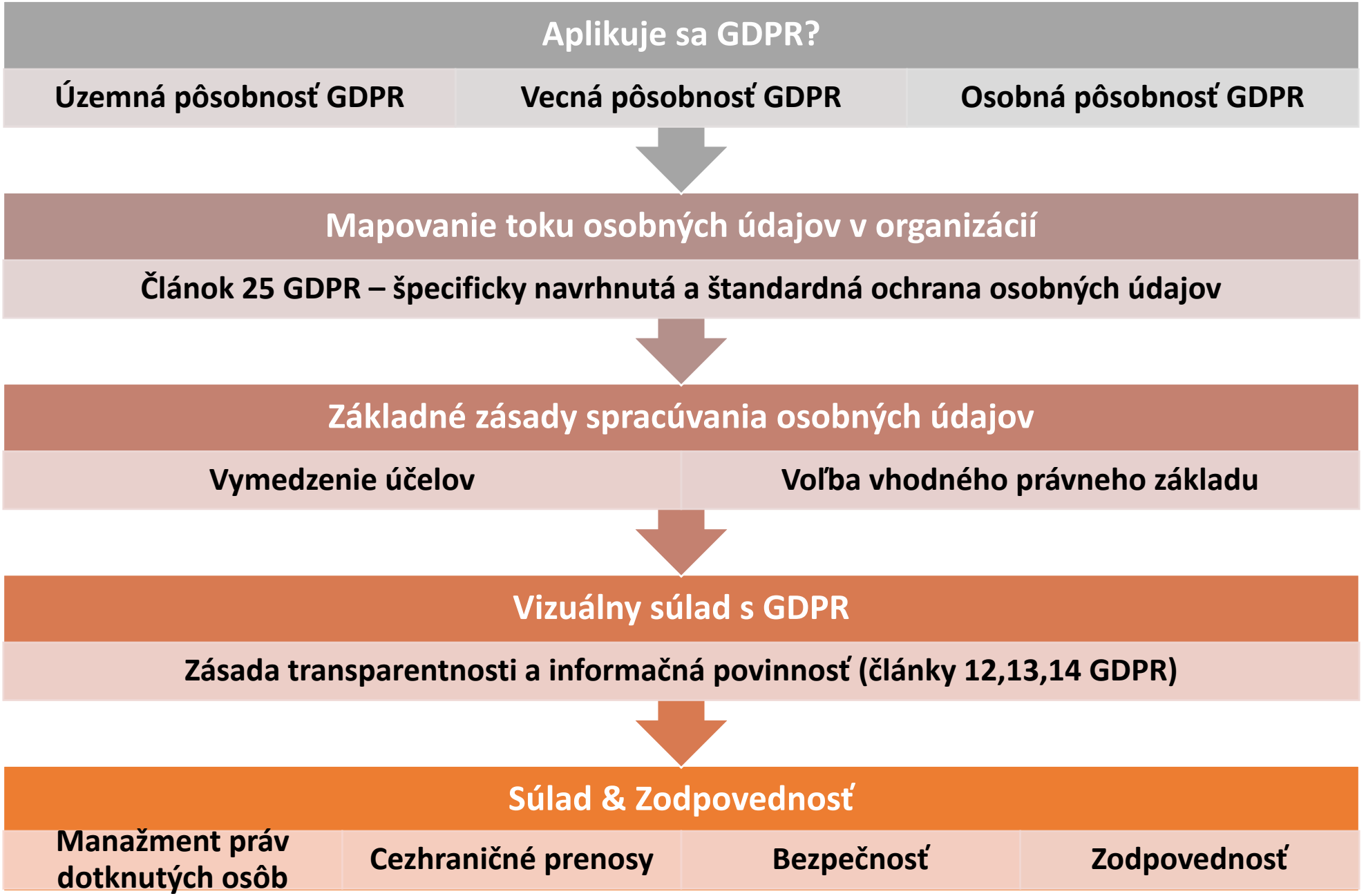
Základné zásady spracúvania

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva

Ochrana osobných údajov
Zimný semester 2020 / 2021
30.10.2020


Aplikuje sa GDPR?
Územná pôsobnosť GDPR
Vecná pôsobnosť GDPR
Osobná pôsobnosť GDPR
Mapovanie toku osobných údajov v organizácií
Článok 25 GDPR – špecificky navrhnutá a štandardná ochrana osobných údajov
Základné zásady spracúvania osobných údajov
Vymedzenie účelov
Voľba vhodného právneho základu
Vizuálny súlad s GDPR
Zásada transparentnosti a informačná povinnosť (články 12,13,14 GDPR)
Súlad & Zodpovednosť
Manažment práv dotknutých osôb
Cezhraničné prenosy
Bezpečnosť
Zodpovednosť

Základné zásady spracúvania osobných údajov

Článok 5 GDPR

- *Zásada zákonnosti, spravodlivosti a transparentnosti (čl. 5 ods. 1 [a])*
- *Zásada obmedzenia účelu (čl. 5 ods. 1 [b])*
- **Zásada minimalizácie údajov (čl. 5 ods. 1 [c])**
- **Zásada správnosti údajov (čl. 5 ods. 1 [d])**
- **Zásada minimalizácie uchovávania (čl. 5 ods. 1 [e])**
- **Zásada integrity a dôvernosti (čl. 5 ods. 1 [f])**
- **Zásada zodpovednosti (čl. 5 ods. 2)**

Zásada zákonnosti

- „Osobné údaje musia byť...spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe“

- Zákonnosť
- Spravodlivosť
- Transparentnosť

Zásada zákonnosti (2)

- **„Osobné údaje musia byť...spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe“**
- Zákonnosť má dve roviny
  - Užšia (Článok 6 GDPR – právne základy a ich právna úprava)
  - **Širšia (Proporcionalita zásahu)**
    - **Článok 8 (2) Dohovoru o ochrane ZĽPaS a Článok 52 (1) Charty základných práv EÚ**

Zásada zákonnosti (2)

- Taylor-Sabori v Spojené kráľovstvo (ESĽP)
- Rotaru v Rumunsko (ESĽP)
- Peck v Spojené kráľovstvo (ESĽP)
- Khelil v Švajčiarsko (ESĽP)
- Digital Rights Ireland proti Minister of Communications (SDEÚ)

Zásada zákonnosti (3)

- **Spravodlivosť**
  - Vzťah prevádzkovateľa (sprostredkovateľa) a dotknutej osoby
  - Aspekt dôvery
  - Spôsob získania
  - Posúdenie vplyvu na jednotlivca

Zásada zákonnosti (4)

- **Transparentnosť**
  - Recitál 39 GDPR
  - Tri základné oblasti transparentnosti
    - Poskytnutie informácií o spracúvaní o dotknutej osobe (Čl. 13-14)
    - Komunikácia výkonu jednotlivých práv (Čl. 15-22)
    - Komunikácia porušenia ochrany osobných údajov (Čl. 34)
  - Článok 12, 13, 14 GDPR

  - Haralambie proti Rumunsku (ESĽP)
  - K.H. a iní proti Slovensku (ESĽP)

Zásada minimalizácie údajov

- „Osobné údaje musia byť...primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú.“

- Záruky
  - Špecificky navrhnutá a štandardná ochrana osobných údajov
  - Pseudonymizácia a anonymizácia

Zásada správnosti

- „Osobné údaje musia byť...správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska **účelov, na ktoré sa spracúvajú**, bezodkladne vymažú alebo opravia“

- Právo na opravu (článok 16 GDPR)
- Právo na vymazanie (článok 17 GDPR)

Zásada minimalizácie uchovávania

- Osobné údaje musia byť...uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac **dovtedy, kým je to potrebné na účely**, na ktoré sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb

Zásada minimalizácie uchovávania (2)

- Berie sa do úvahy:
- (i) súčasná a budúca hodnota spracúvaných údajov, (ii) náklady, riziká a zodpovednosť súvisiacu so spracúvanými údajmi a (iii) potenciálne opatrenia na zaručenie, že údaje sú spracúvané v súlade so zásadou správnosti.

Zásada minimalizácie uchovávania (3)

Účel	Doba uchovávania
Personalistika a mzdy	
Daňové a účtovné účely	
Prezentácia značky v online priestore	
Newsletter	
Ochrana a bezpečnosť majetku	
Poskytovanie Služby	
Štatistické účely	
Archívne účely	

Zásada integrity a dôvernosti (bezpečnosť)

- „Osobné údaje musia byť...spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení.“

Zásada zodpovednosti („Accountability“)

- „Prevádzkovateľ je zodpovedný za súlad s odsekom 1 (Zásady spracúvania) a musí vedieť tento súlad preukázať.“

- a) aktívna a preventívna činnosť prevádzkovateľov (zavedenie opatrení, ktoré zaručia dodržiavanie pravidiel a politík ochrany osobných údajov)
- b) záznamová činnosť prevádzkovateľov (príprava dokumentov, ktoré preukazujú súlad s pravidlami ochrany osobných údajov)

Zásada zodpovednosti („Accountability“)

- **Súčasti (komponenty zásady zodpovednosti**
  1. povinnosť viesť záznamy o spracovateľských operáciách (článok 30)
  2. kooperácia s dozorným orgánom na požiadanie (článok 31)
  3. opatrenia zaručujúce bezpečnosť osobných údajov (článok 32)
  4. oznámenie porušenia ochrany osobných údajov dozornému orgánu / dotknutej osobe (články 33-34)
  5. posúdenie vplyvu na ochranu údajov (článok 35)
  6. predchádzajúca konzultácia s dozorným orgánom (článok 36)
  7. určenie zodpovednej osoby (články 37-39)

Príklad

- Univerzita Komenského v Bratislave prevádzkuje internát pre svojich študentov. Za účelom poskytnutia kvalitných ubytovacích služieb spracúva osobné údaje študentov – ubytovaných. Keďže nemá dostatok peňazí, uzavrie zmluvu so spoločnosťou Red Dull a pošle študentom e-mail s reklamou na jej produkty. Doba uchovávania o študentoch osobných údajov na účel poskytnutia ubytovania je v Politike ochrany súkromia vymedzená na 5 rokov po odubytovaní študenta. Pri ubytovacom oddelení visí na nástenke zoznam všetkých ubytovaných študentov, ktorý obsahuje meno a priezvisko a rodné číslo ubytovaných.
- K osobným údajom má prístup aj vrátnik, ktorý si značí do denníka mená študentiek a neskoro v noci im posiela textové a multimediálne správy.
- Databázu ubytovaných napadli hackeri a referentky študijného oddelenia majú dôvodné obavy, že došlo k úniku osobných údajov ubytovaných. Situáciu sa snažia ututlať.
- Pri výbere spolubývajúcich systém upravuje možnosť „výber partnerskej izby," v ktorej môžu spolu bývať aj páry opačného pohlavia. Zdenka Mokrá sa obáva, že táto informácia odhalí údaje o jej sexuálnom živote.

Transparentnosť / Informačná povinnosť

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva

Ochrana osobných údajov
Zimný semester 2020 / 2021
30.10.2020

Transparentnosť

Informačná povinnosť

Článok 12 GDPR

Prevádzkovateľ prijme vhodné opatrenia s cieľom poskytnúť dotknutej osobe všetky informácie uvedené v článkoch 13 a 14 a všetky oznámenia podľa článkov 15 až 22 a článku 34, ktoré sa týkajú spracúvania, a to **v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho,** a to najmä v prípade informácií určených osobitne dieťaťu. Informácie sa poskytujú písomne alebo inými prostriedkami, vrátane v prípade potreby elektronickými prostriedkami. Ak o to požiadala dotknutá osoba, informácie sa môžu poskytnúť ústne za predpokladu, že sa preukázala totožnosť dotknutej osoby iným spôsobom.

Informačná povinnosť (2)

- Stručne
- Transparentne
- Zrozumiteľne
- Ľahko dostupná forma
- Formulovane jasne a jednoducho

Informačná povinnosť (3)

Univerzita Komenského

Informačná povinnosť

- Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby (čl. 13)
- Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby (čl. 14)

VÝNIMKY!

Informačná povinnosť (4)

- Identita prevádzkovateľa
- Kontakt na zodpovednú osobu
- Účely a právne základy vrátane opisu oprávneného záujmu prípadne či ide o zákonnú alebo zmluvnú požiadavku
- Príjemcovia alebo kategórie príjemcov
- Cezhraničné prenosy
- Doba uchovávania
- Práva dotknutých osôb, právo na odvolanie súhlasu, právo podať sťažnosť dozornému orgánu
- Automatizované individuálne rozhodovanie
- Kategória dotknutých osôb
- Zdroj osobných údajov

Informačná povinnosť (5) - výnimky

- **Ak informáciami už dotknutá osoba disponuje**
- Ak (i) by sa poskytnutie informácií ukázalo ako nemožné alebo by si to vyžadovalo neprimerané úsilie; alebo (ii) pokiaľ je pravdepodobné, že poskytnutie informácii by znemožnilo alebo závažným spôsobom sťažilo dosiahnutie cieľov takéhoto spracúvania.
- Ak to výslovne stanovuje právo EÚ alebo národné právo
- Právna povinnosť zachovania tajomstva alebo mlčanlivosť

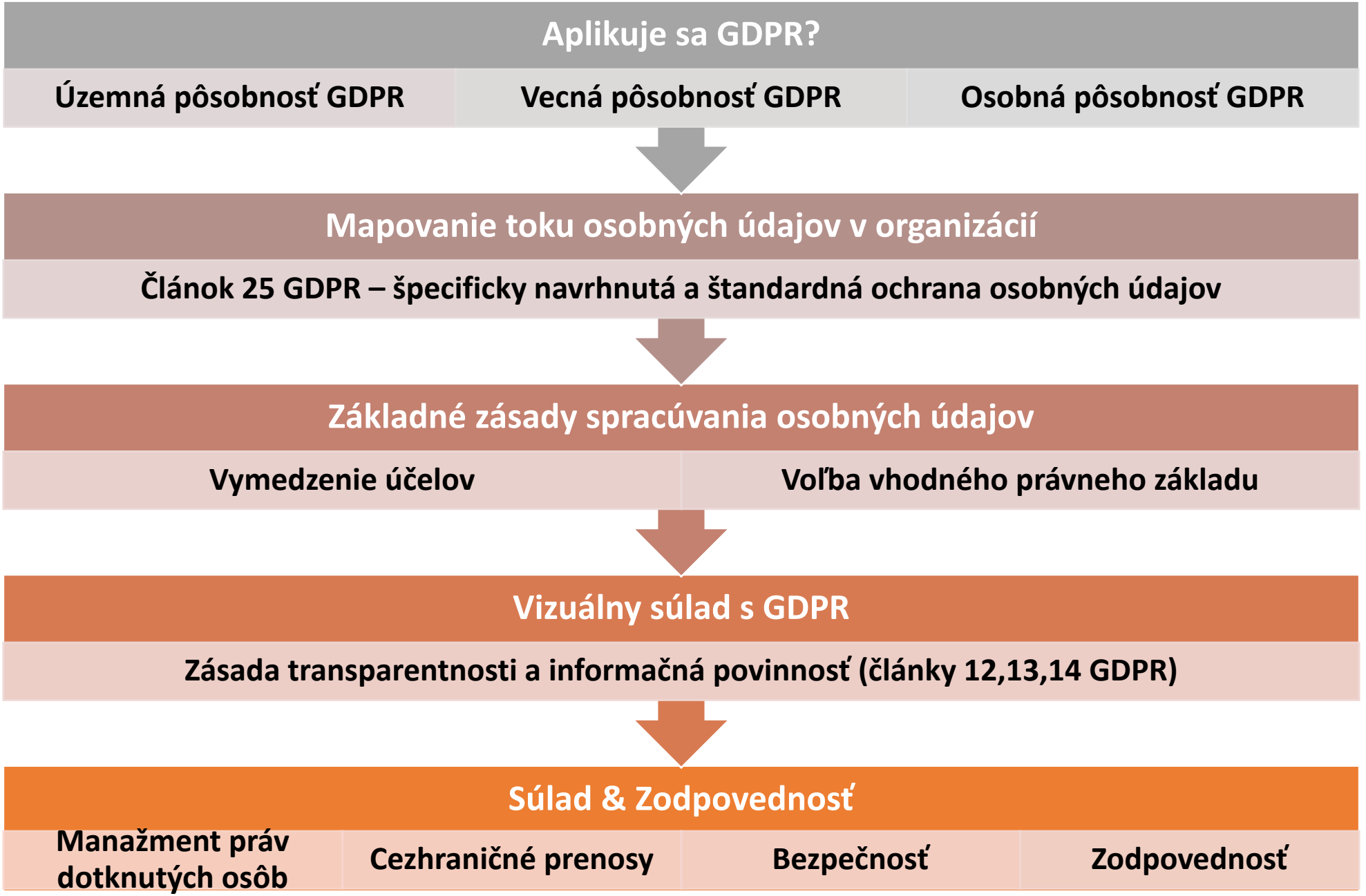
Príklady

- Má prevádzkovateľ povinnosť poskytnúť informácie v prípadoch:
  - Advokát spracúva informácie o svojich klientoch
  - Advokát spracúva informácie o „nečakanom“ svedkovi pre obhajobu
  - Užívateľ sa registruje na sociálnu sieť Facebook
  - Zamestnávateľ monitoruje elektronickú komunikáciu zamestnancov. Musí informovať všetkých adresátov?
  - Súkromný register spracúva údaje z verejne dostupných zdrojov

Práva dotknutých osôb

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva

Ochrana osobných údajov
Zimný semester 2020 / 2021
30.10.2020


Aplikuje sa GDPR?
Územná pôsobnosť GDPR
Vecná pôsobnosť GDPR
Osobná pôsobnosť GDPR
Mapovanie toku osobných údajov v organizácií
Článok 25 GDPR – špecificky navrhnutá a štandardná ochrana osobných údajov
Základné zásady spracúvania osobných údajov
Vymedzenie účelov
Voľba vhodného právneho základu
Vizuálny súlad s GDPR
Zásada transparentnosti a informačná povinnosť (články 12,13,14 GDPR)
Súlad & Zodpovednosť
Manažment práv dotknutých osôb
Cezhraničné prenosy
Bezpečnosť
Zodpovednosť

Právo	Modalita
Právo na informácie	- Ak sa informácie získavajú priamo od dotknutých osôb - Ak sa informácie získavajú inak ako od dotknutých osôb
Právo na prístup	- Potvrdenie - Prístup - Kópia
Právo na opravu	- Opravenie - Doplnenie
Právo na vymazanie	
Právo na obmedzenie spracúvania	
Právo na prenosnosť	- Právo získať údaje - Právo preniesť údaje
Právo namietať	- Právo namietať (verejný alebo oprávnený záujem) - Právo namietať voči priamemu marketingu
Právo nebyť predmetom AIR	- Právo na ľudský zásah - Právo vyjadriť stanovisko - Právo napadnúť rozhodnutie

ZADANIE

- Uplatnite si niektoré z práv dotknutej osoby (15-22 GDPR)
- Pošlite alebo ukážte / dokážte, že ste si ho uplatnili
- **10 bodov**

- 2 obmedzenia
  - Nie voči Univerzite Komenského v Bratislave
  - Nie právo na informácie

- **DO 15.11.2020**

Manažment práv dotknutých osôb

Univerzita Komenského

Prijatie žiadosti / Evidencia

Identifikácia dotknutej osoby

Vybavenie žiadosti

Článok 12 GDPR

Žiadosť dotknutej osoby

OD: veveričiak69@azet.sk
PRE: dpo@superbanka.sk
VEC: Už bolo dosť!

Vy idioti!

Už váz mám dosď! Už stačilo!

Dajte preč tie númerá z mojho učtu inak váz panbožko potrestá!

Novotný

Právo na prístup (článok 15 GDPR)

- Tri roviny:
  - právo na poskytnutie informácií podľa čl. 15 ods. 1 Nariadenia (ktoré sú však takmer identické s informáciami, ktoré sa majú poskytovať podľa čl. 13 a 14 Nariadenia);
  - právo získať prístup k spracúvaným osobným údajom; a
  - právo získať kópiu spracúvaných osobných údajov podľa čl. 15 ods. 3.

2. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

3. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

4. Právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Právo na opravu (článok 16 GDPR)

- Dotknutá osoba má právo na to, aby prevádzkovateľ **bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú**. So zreteľom na účely spracúvania má dotknutá osoba právo na **doplnenie** neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.

- Zásada správnosti
- Právo na obmedzenie spracúvania (čl. 18)

Právo na vymazanie (článok 17 GDPR)

- **1. Dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:**
- **a)** osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
- **b)** dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), a ak neexistuje iný právny základ pre spracúvanie;
- **c)** dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2;
- **d)** osobné údaje sa spracúvali nezákonne;
- **e)** osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;
- **f)** osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1.

Právo na vymazanie (článok 17 GDPR)

- 2. Ak prevádzkovateľ **zverejnil** osobné údaje a podľa odseku 1 je **povinný vymazať** osobné údaje, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení podnikne primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.

- 3. Výnimky

- Google Spain
- **Google proti CNIL (C-507/17)**
- Reálne vynútiteľné právo?

Právo na obmedzenie spracúvania (článok 18 GDPR)

- 1. Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:
- a) dotknutá osoba **napadne správnosť** osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov;
- b) spracúvanie je **protizákonné** a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;
- c) prevádzkovateľ **už nepotrebuje osobné údaje na účely** spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo **obhajovanie právnych nárokov**;
- d) dotknutá osoba namietala voči spracúvaniu podľa článku 21 ods. 1, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.
- 2. Ak sa spracúvanie obmedzilo podľa odseku 1, takéto osobné údaje sa s výnimkou uchovávania spracúvajú **len so súhlasom dotknutej osoby** alebo **na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov**, alebo **na ochranu práv inej fyzickej alebo právnickej osoby**, alebo z **dôvodov dôležitého verejného záujmu** Únie alebo členského štátu.
- 3. Dotknutú osobu, ktorá dosiahla obmedzenie spracúvania podľa odseku 1, prevádzkovateľ **informuje** pred tým, ako bude obmedzenie spracúvania zrušené.

Právo na prenosnosť (článok 20 GDPR)

- 1. **Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi,** v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil, ak:
- a) sa spracúvanie zakladá na súhlase podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), alebo na zmluve podľa článku 6 ods. 1 písm. b), a
- b) ak sa spracúvanie vykonáva automatizovanými prostriedkami.
- **2. Dotknutá osoba má pri uplatňovaní svojho práva na prenosnosť údajov podľa odseku 1 právo na prenos osobných údajov priamo od jedného prevádzkovateľa druhému prevádzkovateľovi, pokiaľ je to technicky možné.**
- 3. Uplatňovaním práva uvedeného v odseku 1 tohto článku nie je dotknutý článok 17. Uvedené právo sa nevzťahuje na spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.
- 4. Právo uvedené v odseku 1 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Právo na prenosnosť (článok 20 GDPR)

- Kedy sa aplikuje?
- Na aké údaje sa vzťahuje?
- Formát?
- Ako prenášať?

Právo na prenosnosť (článok 20 GDPR)

- Zamestnanec a zamestnávateľ
  - Zmluva
  - Pod-účely
    - spracúvanie osobných údajov na účely mzdovej a odvodovej agendy (právny základ: plnenie povinností vyplývajúcich z osobitných predpisov);
    - spracúvanie osobných údajov na účely ďalšieho vzdelávania zamestnancov (právny základ: napr. §140 Zákonníka práce (zvyšovanie kvalifikácie));
    - spracúvanie osobných údajov v rámci hodnotenia splnenia kvalifikačných požiadaviek uchádzača o konkrétnu pracovnú pozíciu (právny základ: čl. 11 Zákonníka práce);
    - spracúvanie osobných údajov o spáchaní trestných činov zamestnancami (ktoré predpokladajú viaceré ustanovenia Zákonníka práce)
    - spracúvanie osobných údajov na účely vydávania stravných lístkov (§152 Zákonníka práce);
    - spracúvanie osobných údajov týkajúce sa hodnotenia výkonnosti zamestnanca (napr. §75 Zákonníka alebo pracovný poriadok);
    - spracúvanie osobných údajov týkajúce monitorovania zamestnancov (oprávnené záujmy zamestnávateľa v spojitosti s §13 Zákonníka práce); a podobne

Právo na prenosnosť (článok 20 GDPR)

- Na aké údaje sa vzťahuje?
  - Priamo poskytnuté údaje
  - Pozorované údaje
  - ~~Odvodené (agregované) údaje~~

Právo na prenosnosť (článok 20 GDPR)

- Dotknutá osoba žiada prenos údajov o jej bankových transakciách poskytovateľovi služby správy financií
- Dotknutá osoba má záujem na získaní histórie počúvaných skladieb od poskytovateľa hudobných streamovacích služieb, aby zistila koľkokrát počúvala konkrétne sklady alebo aby si overila, akú hudbu chce zakúpiť alebo počúvať na inej platforme
- Banka získala údaje od klienta, následne v rámci analytického oddelenia predpovedá jeho budúce správa. Údaje o budúcom správaní klienta?

Právo namietať (článok 21 GDPR)

- **1. Dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané na základe článku 6 ods. 1 písm. e) alebo f) vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.**
- 2. Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, ktoré sa jej týka, na účely takéhoto marketingu, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom.
- 3. Ak dotknutá osoba namieta voči spracúvaniu na účely priameho marketingu, osobné údaje sa už na také účely nesmú spracúvať.
- 4. Dotknutá osoba sa výslovne upozorní na právo uvedené v odsekoch 1 a 2 najneskôr pri prvej komunikácii s ňou, pričom sa toto právo prezentuje jasne a oddelene od akýchkoľvek iných informácií.

Právo nebyť predmetom AIR (článok 22 GDPR)

- **Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.**

- **Automatizované individuálne rozhodovanie**
  - Spracúvanie automatizovanými prostriedkami (vrátane profilovania);
  - Na základe automatizovaného spracúvania sa urobí rozhodnutie;
  - A toto rozhodnutie má právne účinky alebo podobne významné účinky.

Právo nebyť predmetom AIR

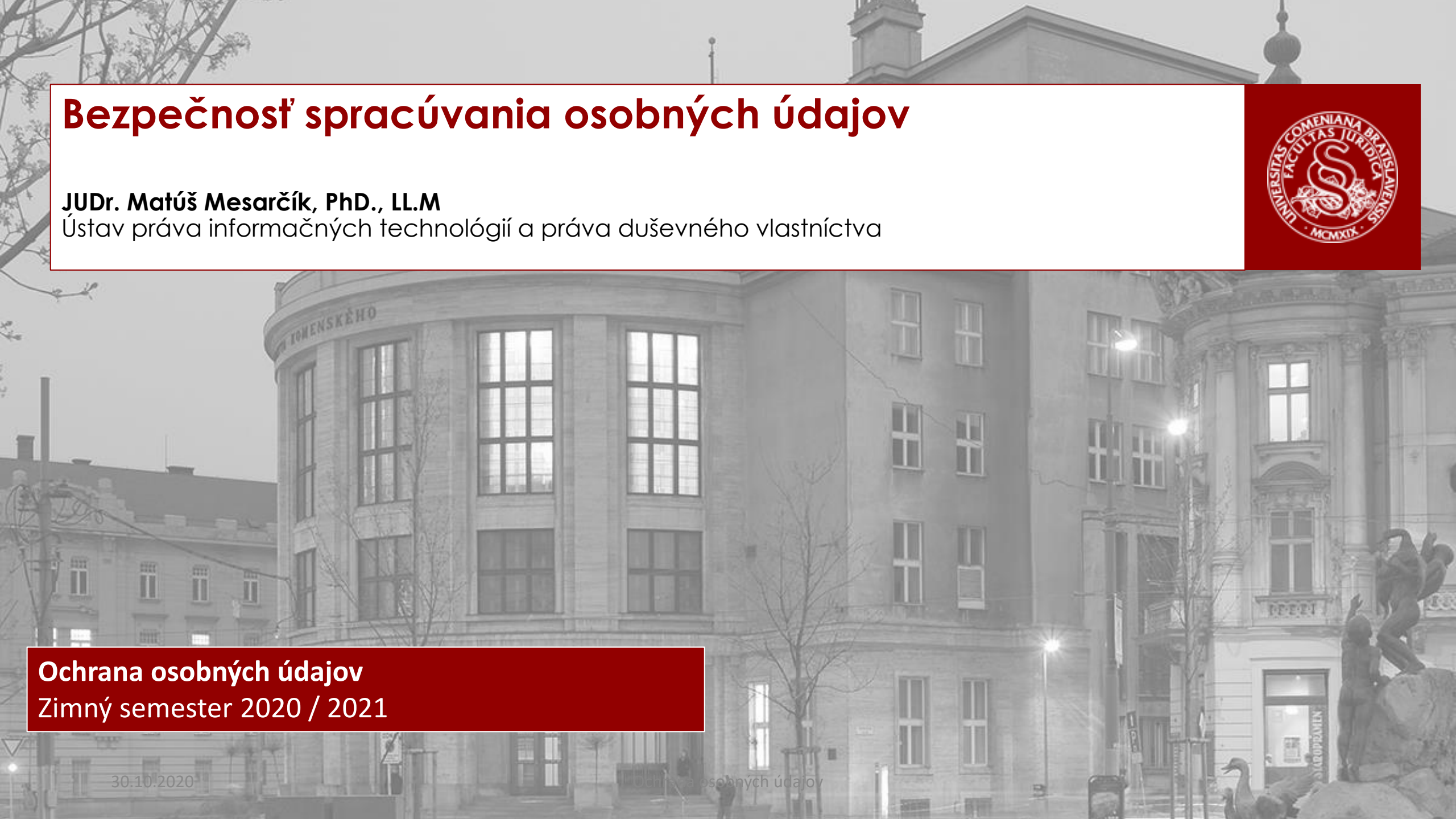
- **Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.**

- **Kedy sa táto situácia vzťahuje na študentov UK?**
- Posudzovanie nároku na ubytovanie
- Kontrola originality záverečnej práce

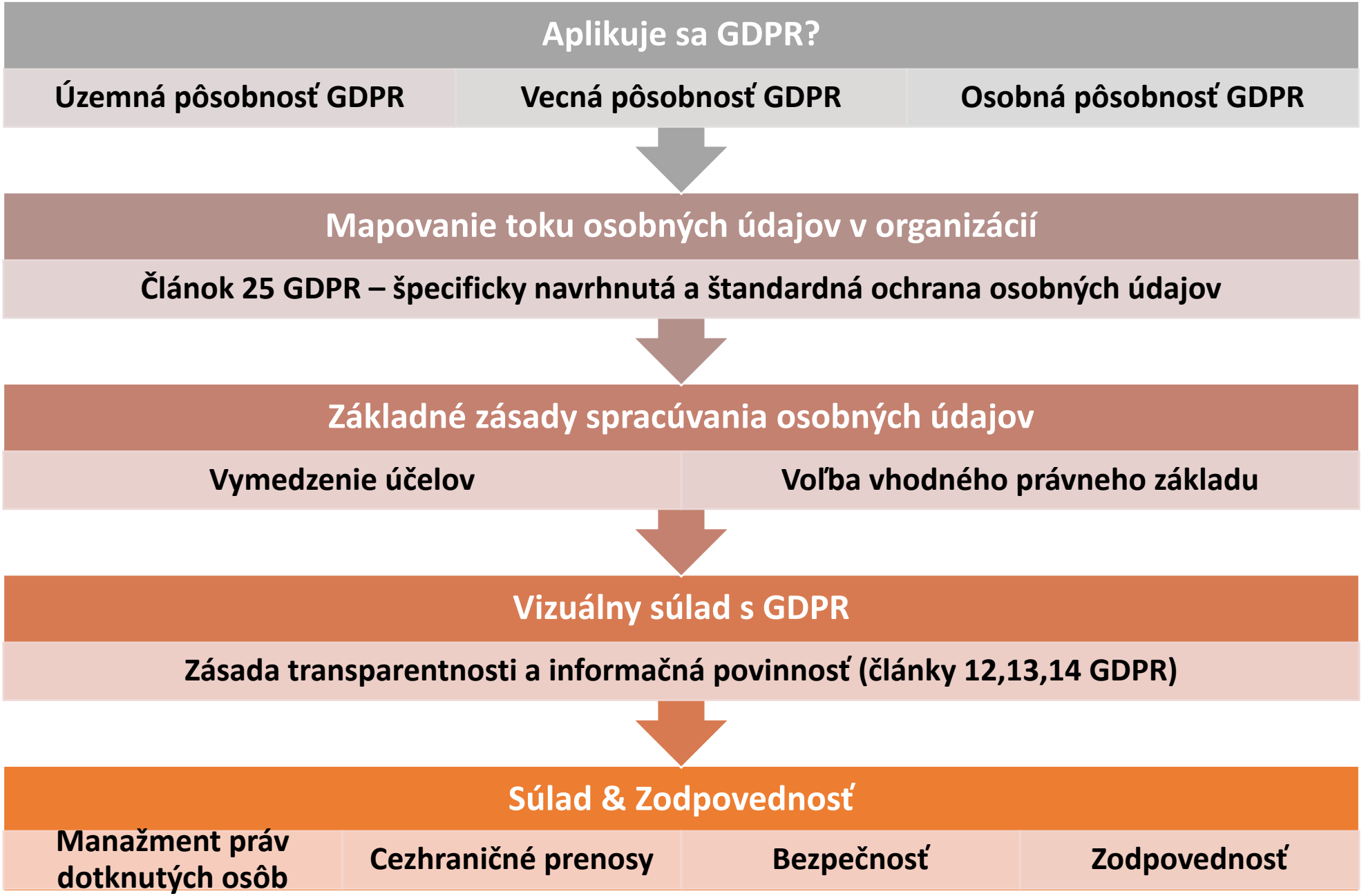
- **Prostriedky obrany:**
  - Právo na ľudský zásah
  - Právo vyjadriť stanovisko
  - Právo napadnúť rozhodnutie

Bezpečnosť spracúvania osobných údajov

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva



Ochrana osobných údajov
Zimný semester 2020 / 2021

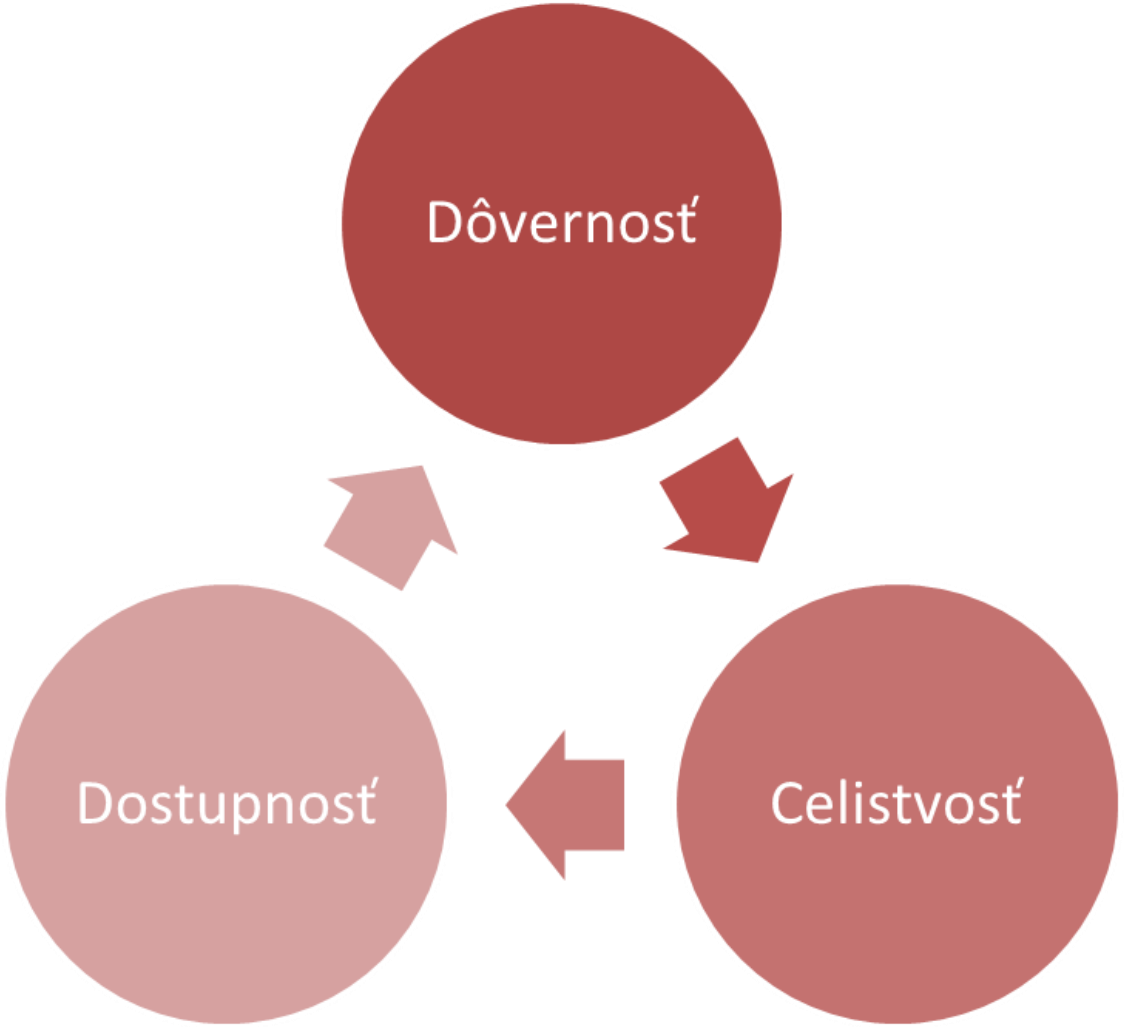

Aplikuje sa GDPR?
Územná pôsobnosť GDPR
Vecná pôsobnosť GDPR
Osobná pôsobnosť GDPR
Mapovanie toku osobných údajov v organizácií
Článok 25 GDPR – špecificky navrhnutá a štandardná ochrana osobných údajov
Základné zásady spracúvania osobných údajov
Vymedzenie účelov
Voľba vhodného právneho základu
Vizuálny súlad s GDPR
Zásada transparentnosti a informačná povinnosť (články 12,13,14 GDPR)
Súlad & Zodpovednosť
Manažment práv dotknutých osôb
Cezhraničné prenosy
Bezpečnosť
Zodpovednosť

Bezpečnosť osobných údajov

- Zásada dôvernosti a integrity
- Princíp technologickej neutrality
- Štandardizácia (ISO normy) = vzťah s GDPR?

- **GDPR = zohľadňovanie subjektívnych rizík!** (Recitál 75)

Bezpečnosť osobných údajov



Článok 32 GDPR

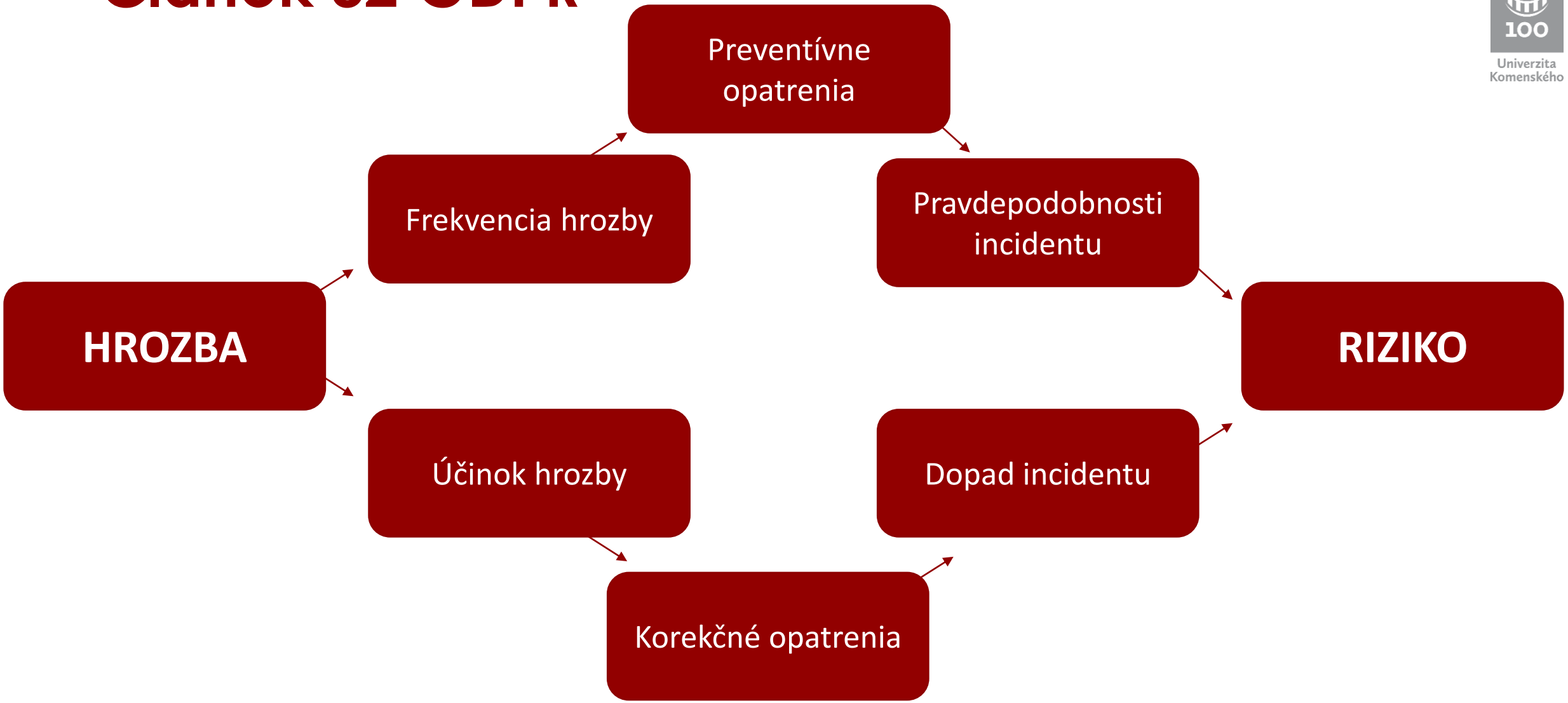
Článok 32

Bezpečnosť spracúvania

- 1. Prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne 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.*

Článok 32 GDPR



Technické a organizačné opatrenia

TECHNICKÉ OPATRENIA

- Postupy bezpečného obstarávania softwarov
- Sieťove firewally
- Monitorovanie bezpečnosti siete
- Manažment identitít
- Šifrovanie alebo pseudonimizácia
- Logovanie
- Ochrana proti malware
- Migrované sieťové úložiská dát
- Záložné kópie dát

Technické a organizačné opatrenia

Univerzita Komenského

ORGANIZAČNĚ OPATRENIA

- Poučenia poverených osôb
- Oddelenie právomocí
- Pravidlá a kontrola vstupu
- Vzdelávanie
- Určenie postupov likvidácie údajov
- Pravidlá manipulácie s nosičmi
- Pravidlá pre používanie prenosných zariadení
- Politika čistého stola
- Organizácia tímu a riadenie bezpečnostných incidentov
- Pravidlá na výber sprostredkovateľov
- Politika manažmentu práv dotknutých osôb

Porušenia ochrany osobných údajov

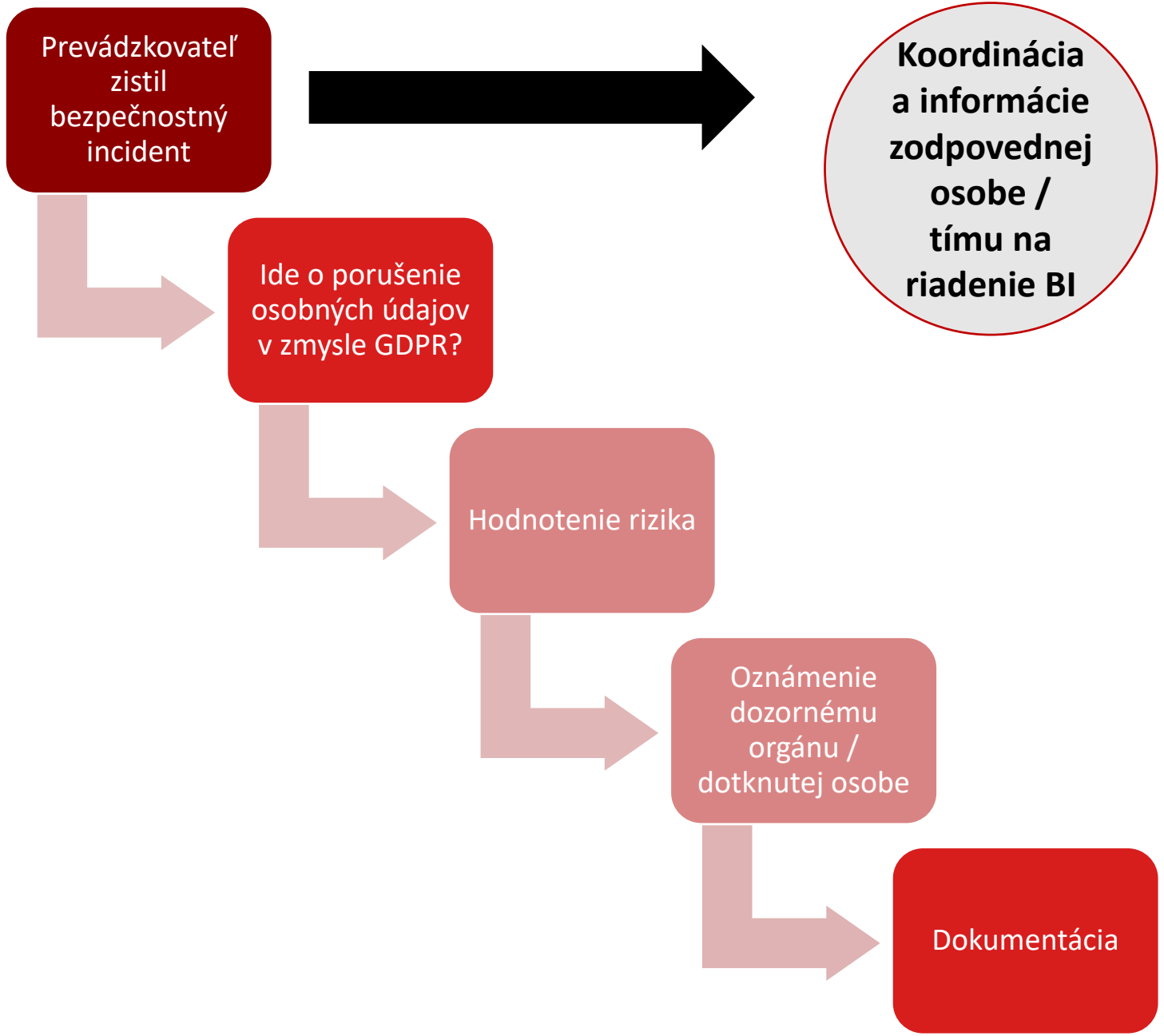
Čl. 4 (12) GDPR **„porušenie ochrany osobných údajov“** je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim

- Porušenie dôvernosti (*confidentiality breach*)
- Porušenie integrity (*integrity breach*)
- Porušenie dostupnosti (*availiability breach*)

Porušenia ochrany osobných údajov

DOZORNÉMU ORGÁNU (Čl. 33)	DOTKNUTEJ OSOBE (Čl. 34)
1. 72 hodín	1. Vysoké riziko = bez zbytočného odkladu
2. Sprostredkovateľ	2. Obsah oznámenia
3. Obsah oznámenia	3. Výnimky
4. Spôsob oznámenia a záznam	4. Intervencia dozorného orgánu

- Čo znamená „*po tom, čo sa o tejto skutočnosti dozvedel*“?
- Ako sa hodnotí, či dochádza k rizikám pre práva a slobody dotknutých osôb?
- Kedy pôjde o „vysoké riziko v zmysle článku 34 ods. 1 GDPR?


Prevádzkovateľ zistil bezpečnostný incident
Koordinácia a informácie zodpovednej osobe / tímu na riadenie BI
Ide o porušenie osobných údajov v zmysle GDPR?
Hodnotenie rizika
Oznámenie dozornému orgánu / dotknutej osobe
Dokumentácia

Porušenia ochrany osobných údajov

Univerzita Komenského

HODNOTENIE (VYSOKÉHO) RIZIKA

- typ porušenia
- povaha, citlivosť a kvantita údajov
- možnosť identifikácie jednotlivcov
- závažnosť dopadu pre jednotlivcov
- deti a zraniteľné osoby
- rola prevádzkovateľa
- počet zasiahnutých osôb
- ostatné faktory

Guidelines on Personal data breach notification under Regulation 2016/679

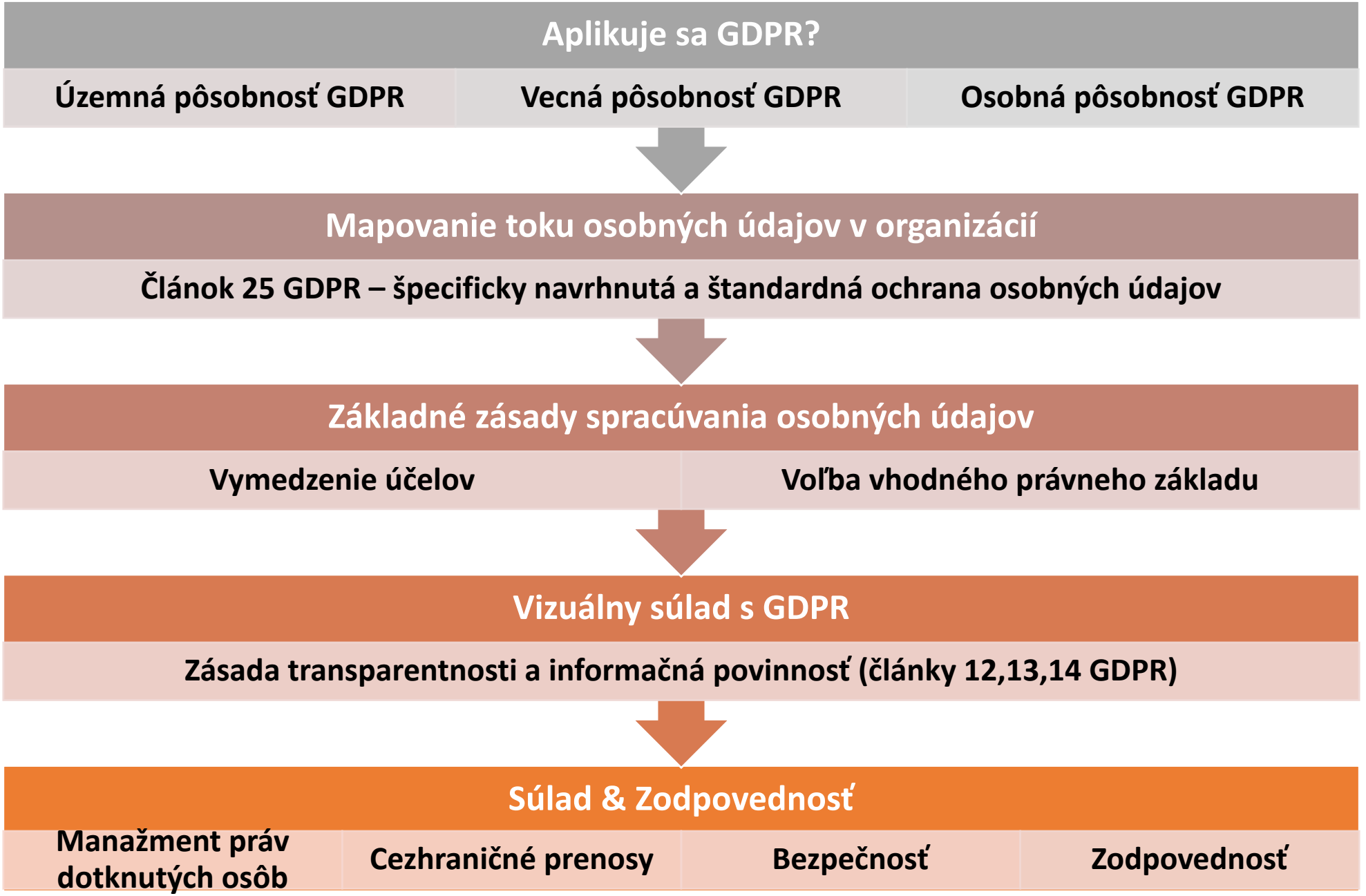
Porušenia ochrany osobných údajov - príklady

- Zamestnancovi prevádzkovateľa bol odcudzený pracovný laptop, v ktorom bolo uložené veľké množstvo citlivých osobných údajov. Pevný disk bol zašifrovaný a kľúč potrebný k dešifrovaniu má iba zamestnanec a jeho šéf.
- Prevádzkovateľ prevádzkuje mobilné aplikácie, ktoré užívateľom umožňuje drobné nákupy. Pre tento účel aplikácia ukladá na zabezpečený server do databázy údajov o platobných kartách užívateľov. Prevádzkovateľ zistí, že došlo k neoprávnenému vstupu tretej osoby do databázy.
- Advokátovi zmizne z kancelárie celý spis týkajúci sa trestného konania jedného z klientov, ktorý je podozrivý z daňových podvodov.

Zodpovednosť pri spracúvaní osobných údajov

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva

Ochrana osobných údajov
Zimný semester 2020 / 2021


Aplikuje sa GDPR?
Územná pôsobnosť GDPR
Vecná pôsobnosť GDPR
Osobná pôsobnosť GDPR
Mapovanie toku osobných údajov v organizácií
Článok 25 GDPR – špecificky navrhnutá a štandardná ochrana osobných údajov
Základné zásady spracúvania osobných údajov
Vymedzenie účelov
Voľba vhodného právneho základu
Vizuálny súlad s GDPR
Zásada transparentnosti a informačná povinnosť (články 12,13,14 GDPR)
Súlad & Zodpovednosť
Manažment práv dotknutých osôb
Cezhraničné prenosy
Bezpečnosť
Zodpovednosť

Zodpovednosť

- Posúdenie vplyvu (článok 35 GDPR);
- Zodpovedná osoba (články 37 – 39 GDPR);
- Predchádzajúca konzultácia (článok 36 GDPR);
- Vypracovanie záznamov o spracovateľských činnostiach (článok 30 GDPR);

- *Kódexy správania*

Posúdenie vplyvu

Univerzita Komenského

Článok 35

Posúdenie vplyvu

Ak typ spracúvania, **najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb**, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie.

Posúdenie vplyvu

- **KEDY?**

  Posúdenie vplyvu na ochranu údajov uvedené v odseku 1 sa vyžaduje najmä v prípadoch:

  – **a)** systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;

  – **b)** spracúvania vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, alebo

  – **c)** systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

  – **d)** ak to určí dozorný orgán

Posúdenie vplyvu

- **KRITÉRIA VYSOKÉHO RIZIKA**
- a) Vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby
- b) Automatizované rozhodovanie s právnym alebo podobne závažným účinkom
- c) Systematické monitorovanie osobných údajov
- d) Spracúvanie citlivých osobných údajov
- e) Spracúvanie údajov vo veľkom rozsahu
- f) Spájanie alebo kombinovanie súborov a údajov pochádzajúcich z rôznych spracovateľských operácií
- g) Spracúvanie údajov týkajúcich sa „zraniteľných“ dotknutých osôb
- h) Využitie nových technológií, technologických alebo organizačných riešení a postupov
- i) Spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu

2 kritéria stačia!

Posúdenie vplyvu

- **Členské štáty mali do 25.5.2018 uverejniť spracovateľské operácie, ktoré podliehajú vykonaniu posúdenia vplyvu**
- **ÚOOÚ SR:**

1. Spracúvanie biometrických údajov fyzických osôb na účely individuálnej identifikácie fyzickej osoby v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248.
2. Spracúvanie genetických údajov fyzických osôb v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248.
3. Spracúvanie lokalizačných údajov v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248.
4. Spracovateľské operácie vykonávané podľa čl. 14 všeobecného nariadenia o ochrane údajov
5. Hodnotenie alebo prideľovanie bodov
6. Posúdenie dôveryhodnosti.
7. Posúdenie platobnej schopnosti.
8. Profilovanie
9. Monitoring práce zamestnanca na základe vážnych dôvodov vyplývajúcich z osobitnej povahy činnosti zamestnávateľa

Posúdenie vplyvu

- **Členské štáty mali do 25.5.2018 uverejniť spracovateľské operácie, ktoré podliehajú vykonaniu posúdenia vplyvu**
- **ÚOOÚ SR:**

10. Spracúvanie osobných údajov na účely vedeckého alebo historického výskumu bez súhlasu dotknutej osoby v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248.

11. Spracovateľské operácie využívajúce nové alebo inovatívne technológie v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248.

12. Systematické kamerové monitorovanie verejných priestorov.

13. Sledovanie osôb súkromnými detektívnymi, resp. bezpečnostnými službami.

Posúdenie vplyvu

- **AKO?**
  - Systematický opis plánovaných spracovateľských operácií a účelu spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ.
  - Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu.
  - Posúdenie rizika pre práva a slobody dotknutých osôb uvedeného v odseku článku 35 ods. 1 Nariadenia.
  - Opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

Posúdenie vplyvu

- Nemocnica spracúva osobné údaje o zdravotnom stave svojich pacientov.
- Spoločnosť, ktorá predáva dopravné systémy sa rozhodla vytvoriť software, ktorý dokáže z kamier nainštalovaných na diaľniciach a vyčleniť a sledovať jednotlivé automobily na základe skenovaniach ich ŠPZ.
- E-shop zobrazuje svojim návštevníkom reklamy na základe ich histórie objednávok.
- Politická strana prostredníctvom algoritmu spracúva osobné údaje získané zo sociálnych sietí na účely politického marketingu?

Cvičenie

- Politická strana prostredníctvom algoritmu spracúva osobné údaje získané zo sociálnych sietí na účely politického marketingu?

Zodpovedná osoba

Univerzita Komenského

Článok 37

Určenie zodpovednej osoby

1. Prevádzkovateľ a sprostredkovateľ určia zodpovednú osobu v každom prípade, keď:

a) spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci;

b) **hlavnými činnosťami** prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo

c) **hlavnými činnosťami** prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov podľa článku 9 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10.

Zodpovedná osoba

- Hlavná činnosť nemocnice je poskytovanie zdravotníckej starostlivosti. Potrebuje spracúvať citlivé osobné údaje?
- Súkromná bezpečnostná agentúra vykonáva dohľad nad verejnými priestormi v niektorých centrách prostredníctvom CCTV?
- Nemocnica spracúva osobné údaje svojich zamestnancov pre účely vyplácania mzdy a pre výkon iných práv a povinností vyplývajúcich z pracovného práva?
- Telekomunikačný operátor spracúva osobné údaje užívateľov telekomunikačnej siete?
- Výskumná spoločnosť vykonáva testy DNA na vzorke 50 000 ľudí ročne?

Zodpovedná osoba

Cvičenie

Váš klient je nádejný start-up, ktorý vymyslel aplikáciu na zobrazovanie reklamy podľa polohy užívateľa. Aplikácia využíva technológiu strojového učenia (*machine learning)*. V praxi to funguje tak, že aplikácia zbiera údaje o polohe zariadenia užívateľa a následne ukazuje užívateľovi ponuky tovarov, v ktorých blízkosti sa nachádza.

1. Má klient povinnosť vykonať posúdenie vplyvu?
2. Má klient povinnosť poveriť do funkcie zodpovednú osobu?

Záznamy o spracovateľských operáciách

- Všeobecná povinnosť viesť záznamy o spracovateľských operáciách (článok 30 ods. 1)
- Výnimky (článok 30 ods. 5);
- Obsah (30 ods. 1 a-g);
- Úrad na ochranu osobných údajov zverejnil vzor na svojom webovom sídle

Záznamy o spracovateľských operáciách

Účel	Právny základ	Kategórie dotknutých osôb	Kategórie osobných údajov	Lehota na výmaz	Kategórie príjemcov	Tretia krajina / medzinárodná organizácia	Bezpečnostné opatrenia
Personalistika mzdy	Plnenie zmluvy (článok 6 ods. 1 písm. b GDPR) a zákonná povinnosť (článok 6 ods. 1 písm. c) GDPR)	Zamestnanci, príbuzní zamestnancov,	Identifikačné osobné údaje, číslo účtu, rodinný stav...	Počas trvania pracovného pomeru a uplynutí zákonných lehôt pre uchovávanie určitých typov dokumentov (spravidla 5 až 10 rokov, v niektorých prípadoch až 70 rokov od narodenia zamestnanca).	Zamestnanci, poverené osoby, daňové úrady, sociálana poisťovňa, zdravotná poisťovňa	USA – Privacy Shield	Antivirus, firewall, logy, dvofázová autentifikácia
Politický marketing (profilovanie)							

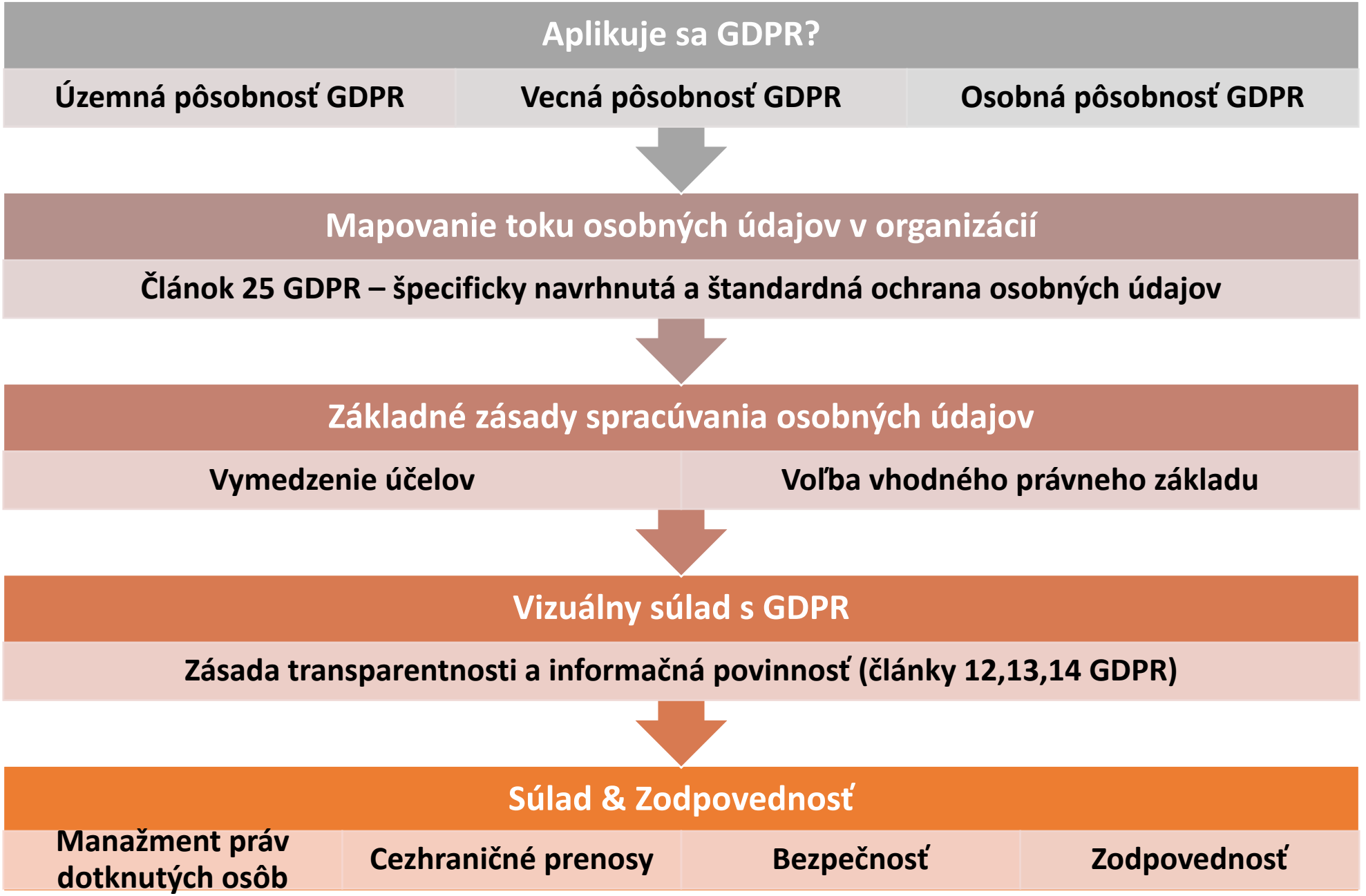
Kódexy správania

- Samoregulačný nástroj pre združenia;
- Cieľom je zefektívniť uplatňovanie GDPR, pričom sa vezmú do úvahy osobitné črty rôznych sektorov spracúvania a osobitné potreby mikropodnikov a malých a stredných podnikov;
- Kódexy sa schvaľujú dozorným orgánom v rámci správneho konania.

Cezhraničné prenosy osobných údajov

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva

Ochrana osobných údajov
Zimný semester 2019 / 2020


Aplikuje sa GDPR?
Územná pôsobnosť GDPR
Vecná pôsobnosť GDPR
Osobná pôsobnosť GDPR
Mapovanie toku osobných údajov v organizácií
Článok 25 GDPR – špecificky navrhnutá a štandardná ochrana osobných údajov
Základné zásady spracúvania osobných údajov
Vymedzenie účelov
Voľba vhodného právneho základu
Vizuálny súlad s GDPR
Zásada transparentnosti a informačná povinnosť (články 12,13,14 GDPR)
Súlad & Zodpovednosť
Manažment práv dotknutých osôb
Cezhraničné prenosy
Bezpečnosť
Zodpovednosť

Modely ochrany osobných údajov vo svete

Model	Charakteristika	Krajina
Komplexný	- Komplexná právna úprava - Pokrýva verejný aj súkromný sektor - Dozorné orgány	Európska únia
Sektorový	- Absencia všeobecného právneho predpisu - Regulácia jednotlivých odvetví	USA/Japonsko
Samoregulačný	- Absencia všeobecného právneho predpisu - Sektorové normy alebo kódexy	Singapur
Spoločná regulácia	- Základný právny rámec - Sektorové normy	Kanada

Kedy ide o cezhraničné prenosy?

- Zamestnanec slovenskej firmy ide na služobnú cestu do Vietnamu a odtiaľ cez vzdialený prístup vstúpiť do databázy klientov?
- Zamestnanec slovenskej firmy pošle profily klientov do firmy sídliacej vo Vietname?

Postup

- Prevádzkovateľ chce exportovať osobné údaje do Číny, aký právny základ musí hľadať?
    1. Je krajina v EÚ / EHS?
    2. Poskytuje tretia krajina primeranú úroveň ochrany?
    3. Viem použiť primerané záruky?
    4. Viem použiť výnimku pre cezhraničný prenos?

- Existuje špecifické medzinárodné dojednanie?

Cezhraničné prenosy

- Základné pravidlo: voľný pohyb osobných údajov po EÚ

Rozhodnutie o primeranosti

Článok 45: *„prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môže uskutočniť, ak Komisia rozhodla, že tretia krajina, územie alebo jeden či viaceré určené sektory v danej tretej krajine alebo predmetná medzinárodná organizácia zaručujú primeranú úroveň ochrany...na takýto prenos nie je nutné žiadne osobitné povolenie.“*

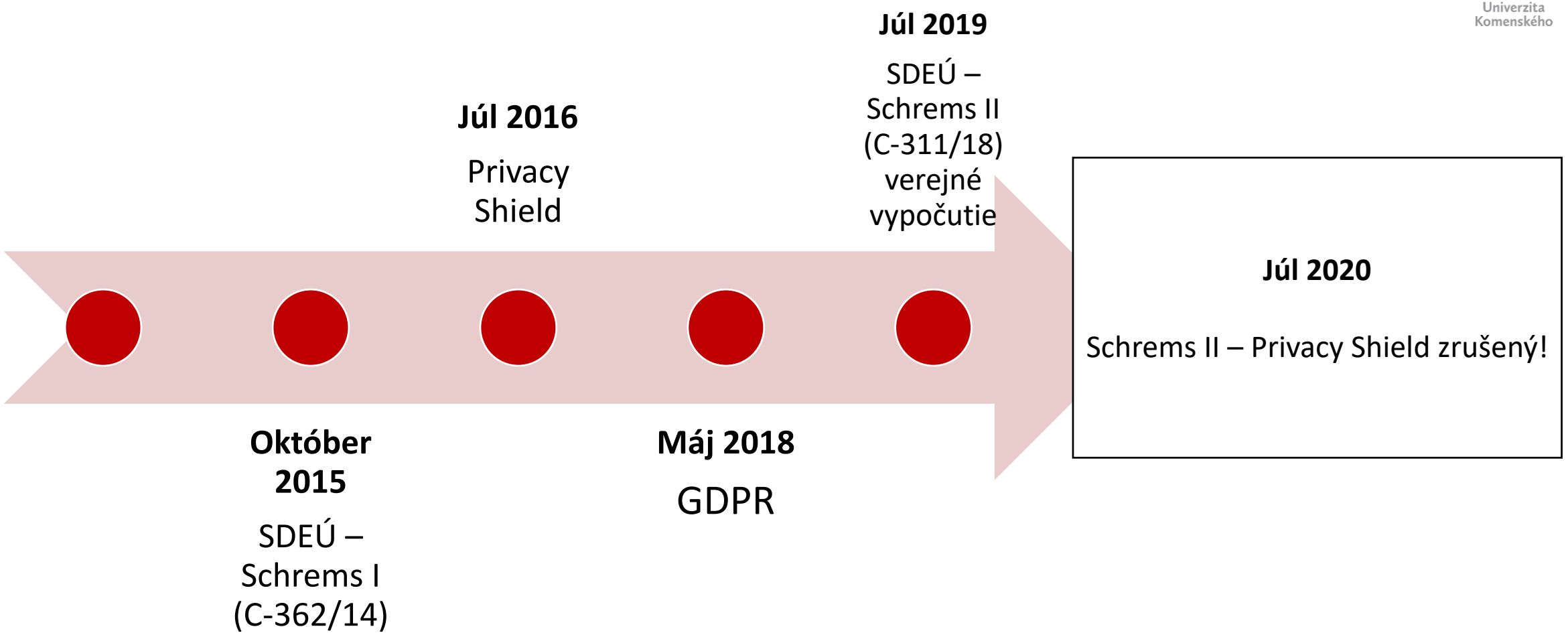
Rozhodnutie o primeranosti

- Komitológia
- Posudzované faktory:
    - Právny štát, dodržiavanie ZĽPaSm bezpečnosť, prístup OVM
    - Dozorný orgán
    - Medzinárodné záväzky

Rozhodnutie o primeranosti

- Andorrské kniežatstvo
- Argentína
- Faerské ostrovy
- Guernsey
- Izrael
- Japonsko
- Jersey
- Nový Zéland
- Kanada (komerčné organizácie)
- Ostrov Man
- Švajčiarsko
- Uruguajská východná republika
- ~~Spojené štáty americké (spoločnosti certifikované v režime Privacy Shield)~~

Rozhodnutie o primeranosti – USA



Primerané záruky

- a) **právne záväzný a vykonateľný nástroj medzi orgánmi verejnej moci** alebo verejnoprávnymi subjektmi
- b) **záväzné vnútropodnikové pravidlá** v súlade s článkom 47;
- c) **štandardné doložky o ochrane údajov**, ktoré prijala **Komisia** v súlade s postupom preskúmania uvedeným v článku 93 ods. 2;
- d) **štandardné doložky o ochrane údajov**, ktoré prijal **dozorný orgán**, a ktoré schválila Komisia podľa postupu preskúmania uvedeného v článku 93 ods. 2;
- e) schválený **kódex správania** podľa článku 40 spolu so záväznými a vymáhateľnými záväzkami prevádzkovateľa alebo sprostredkovateľa v tretej krajine spočívajúcimi v uplatňovaní primeraných záruk, a to aj pokiaľ ide o práva dotknutých osôb, alebo
- f) schválený **certifikačný mechanizmus** podľa článku 42 spolu so záväzným a vymáhateľným záväzkom prevádzkovateľa alebo sprostredkovateľa v tretej krajine spočívajúcim v uplatňovaní primeraných záruk, a to aj pokiaľ ide o práva dotknutých osôb.

Osobitné medzinárodne dojednania

- Rozhodnutie Rady 2012/472/EÚ z 26. apríla 2012 o uzavretí Dohody medzi Spojenými štátmi americkými a Európskou úniou o využívaní osobných záznamov o cestujúcich a ich postupovaní Ministerstvu vnútornej bezpečnosti Spojených štátov amerických, Ú. v. EÚ L 215/4, 2012. Text dohody je priložený k rozhodnutiu, Ú. v. EÚ L 215, 2012, s. 5 – 14.
- Rozhodnutie Rady 2010/412/EÚ z 13. Júla 2010 o uzavretí Dohody medzi Európskou úniou a Spojenými štátmi americkými o spracovaní a zasielaní údajov obsiahnutých vo finančných správach z Európskej únie do Spojených štátov amerických na účely Programu na sledovanie financovania terorizmu, Ú. v. EÚ L 195, 2010, s. 5 – 14.

Záväzné vnútropodnikové pravidlá (BCR)

- Pre skupiny podnikov
- Materiálne podmienky (čl. 47 ods.1)
- Formálne podmienky (čl. 47 ods.2)

Príklady doložiek

- Dozorný orgán
- Komisia

- Prevádzkovateľ – prevádzkovateľ (3. krajina)
- Prevádzkovateľ – sprostredkovateľ (3. krajina)

Výnimky pre osobitné situácie

- dotknutá osoba vyjadrila **výslovný súhlas** s navrhovaným prenosom po tom, ako bola informovaná o rizikách, ktoré takéto prenosy môžu pre ňu predstavovať z dôvodu absencie rozhodnutia o primeranosti a primeraných záruk
- prenos je nevyhnutný **na plnenie zmluvy** medzi dotknutou osobou a prevádzkovateľom alebo na vykonanie predzmluvných opatrení prijatých **na žiadosť dotknutej osoby**;
- prenos je nevyhnutný pre **uzatvorenie alebo plnenie zmluvy uzatvorenej v záujme** dotknutej osoby medzi prevádzkovateľom a inou fyzickou alebo právnickou osobou;
- prenos je nevyhnutný **z dôležitých dôvodov verejného záujmu**;
- prenos je nevyhnutný na **preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov**;
- prenos je nevyhnutný na ochranu **životne dôležitých záujmov dotknutej osoby** alebo iných osôb, ak je dotknutá osoba fyzicky alebo **právne nespôsobilá vyjadriť súhlas**;
- prenos sa uskutočňuje z **registra**, ktorý je podľa práva Únie alebo práva členského štátu určený na **poskytovanie informácií verejnosti a ktorý je otvorený na nahliadanie verejnosti alebo akejkoľvek** osobe, ktorá vie preukázať oprávnený záujem, ale len pokiaľ sú v tomto konkrétnom prípade splnené podmienky stanovené právom Únie alebo právom členského štátu na nahliadanie.
- **závažné oprávnené záujmy** prevádzkovateľa.

Rozhodnutia súdov tretích krajín

Článok 48

Prenosy alebo poskytovanie údajov, ktoré právo Únie nepovoľuje

Akýkoľvek **rozsudok súdu alebo tribunálu** a akékoľvek **rozhodnutie správneho orgánu tretej krajiny**, ktorým sa od prevádzkovateľa alebo sprostredkovateľa vyžaduje preniesť alebo poskytnúť osobné údaje, môže byť uznané alebo vykonateľné akýmkoľvek spôsobom **len vtedy, ak sa zakladá na medzinárodnej dohode**, ako napríklad zmluve o vzájomnej právnej pomoci, platnej medzi žiadajúcou treťou krajinou a Úniou alebo členským štátom bez toho, aby boli dotknuté iné dôvody prenosu podľa tejto kapitoly.

Microsoft case (USA)

*CLOUD Act (The **C**larifying **L**awful **O**verseas **U**se of **D**ata Act)*

Prípad

- **Wakanda, malý štát umiestnený v strednej Afrike nečakane odhalil svoju existenciu svetu. Čo bolo považované za krajinu pastierov, je v súčasnosti jednou z technologicky najvyspelejších krajín sveta. Množstvo spoločností z Európskej únie by chcelo vykonať do tejto krajiny na pravidelnej báze vykonávať cezhraničné prenosy osobných údajov.**
- A) Išlo by v tomto prípade o cezhraničný prenos?
- B) Aké faktory by posudzovala Európska komisia pri vyhodnocovaní, či Wakanda poskytuje primeranú úroveň ochrany?
- C) Čo v prípade, ak by vo Wakande prebehla občianska vojna a bola by nastolená vojenská diktatúra miestne armády?

Prípad

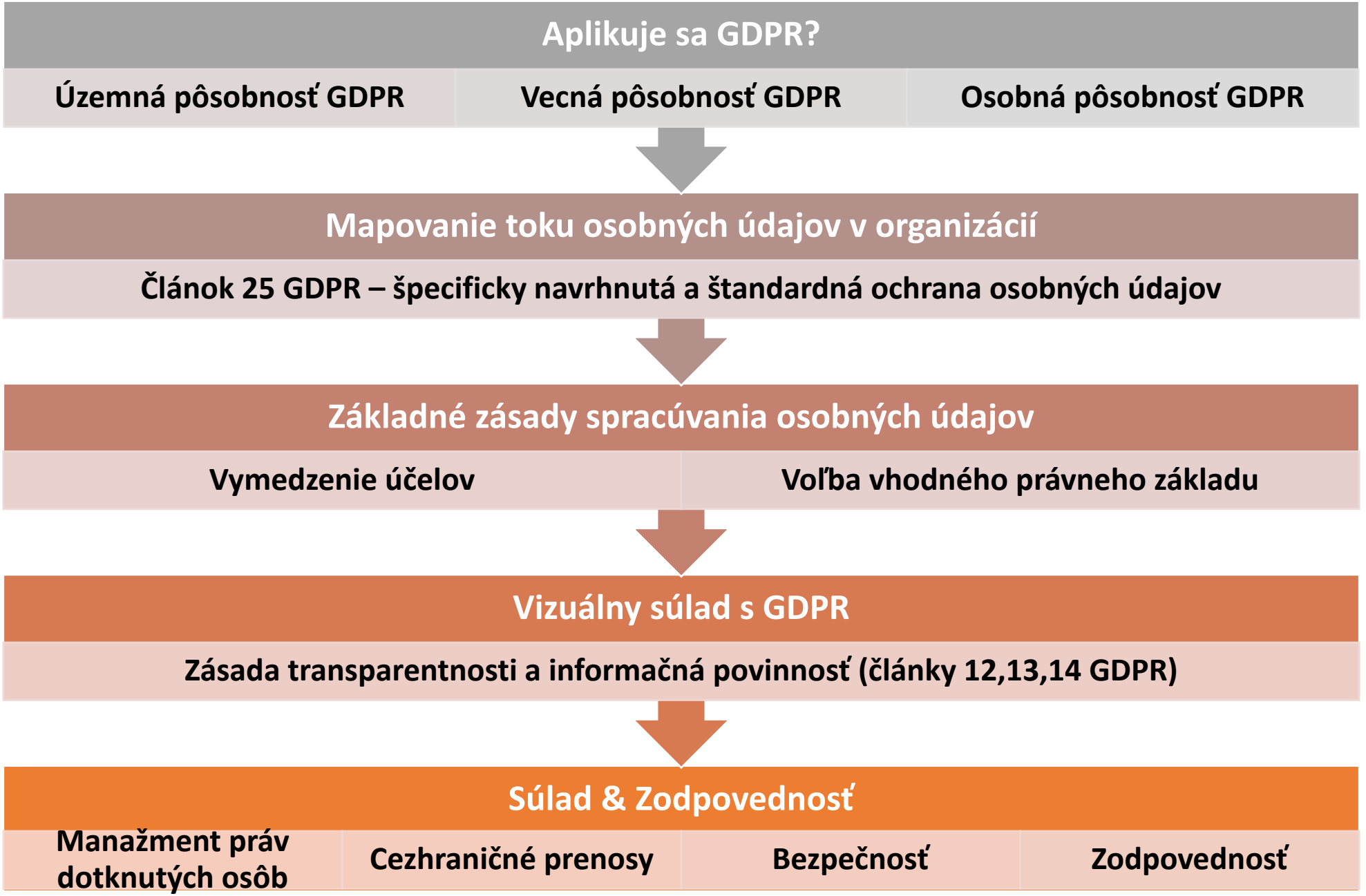
Univerzita Komenského poskytuj svojim študentom možnosť zúčastniť sa výmenného pobytu v USA na vybraných amerických univerzitách. V rámci komunikácie medzi UK a univerzitami v USA sú osobné údaje vybraných študentov UK prenášané do USA.

A) Ide v tomto prípade o cezhraničný prenos?
B) Ak áno, ktorý právny základ pre cezhraničný prenos by ste odporučili UK? Svoju odpoveď odôvodnite.

Dozorné orgány a zodpovednosť

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva

Ochrana osobných údajov
Zimný semester 2020 / 2021


Aplikuje sa GDPR?
Územná pôsobnosť GDPR
Vecná pôsobnosť GDPR
Osobná pôsobnosť GDPR
Mapovanie toku osobných údajov v organizácií
Článok 25 GDPR – špecificky navrhnutá a štandardná ochrana osobných údajov
Základné zásady spracúvania osobných údajov
Vymedzenie účelov
Voľba vhodného právneho základu
Vizuálny súlad s GDPR
Zásada transparentnosti a informačná povinnosť (články 12,13,14 GDPR)
Súlad & Zodpovednosť
Manažment práv dotknutých osôb
Cezhraničné prenosy
Bezpečnosť
Zodpovednosť

Postavenie dozorného orgánu

Univerzita Komenského

Článok 51

Dozorný orgán

- 1. Každý členský štát stanoví, že za monitorovanie uplatňovania tohto nariadenia je zodpovedný jeden alebo viacero nezávislých orgánov verejnej moci s cieľom chrániť základné práva a slobody fyzických osôb pri spracúvaní a uľahčiť voľný tok osobných údajov v rámci Únie (ďalej len „dozorný orgán“).
- 2. Každý dozorný orgán prispieva ku konzistentnému uplatňovaniu tohto nariadenia v celej Únii. Na tento účel dozorné orgány spolupracujú navzájom, ako aj s Komisiou v súlade s kapitolou VII.
- 3. Ak je v členskom štáte zriadený viac než jeden dozorný orgán, tento členský štát určí dozorný orgán, ktorý má zastupovať uvedené orgány vo výbore, a stanoví mechanizmus na zabezpečenie súladu zo strany ostatných orgánov s pravidlami týkajúcimi sa mechanizmu konzistentnosti uvedeného v článku 63.
- 4. Každý členský štát oznámi Komisii ustanovenia svojho práva, ktoré prijme podľa tejto kapitoly, do 25. mája 2018 a bezodkladne oznámi všetky následné zmeny, ktoré sa týkajú týchto ustanovení.

Nezávislosť

Univerzita Komenského

Článok 52

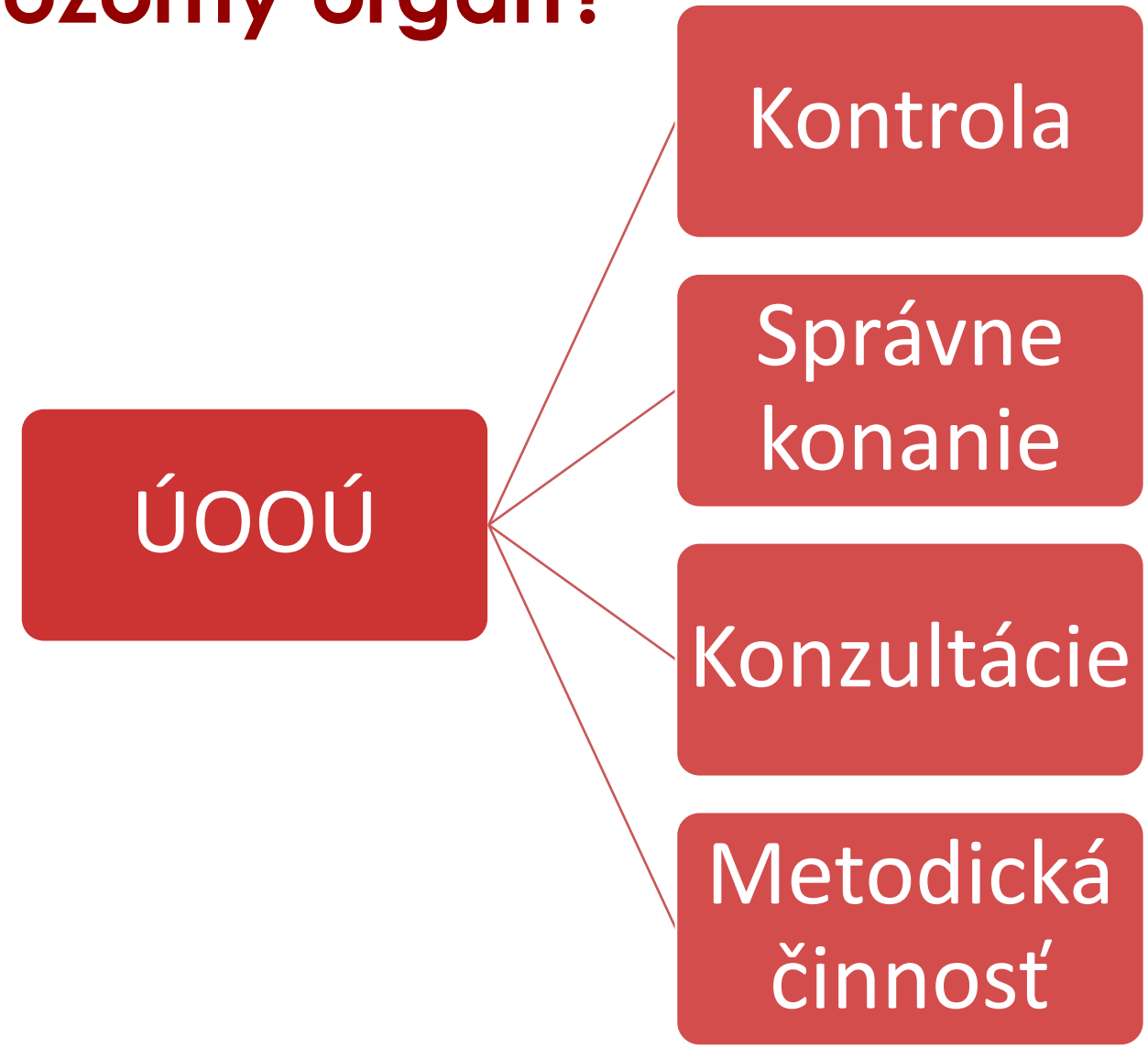
Nezávislosť

1. Každý dozorný orgán koná pri plnení svojich úloh a výkone svojich právomocí v súlade s týmto nariadením **úplne nezávisle.**
2. Člen alebo členovia dozorného orgánu nesmú byť pri plnení svojich úloh a výkone svojich právomocí podľa tohto nariadenia **pod vonkajším vplyvom,** či už priamym alebo nepriamym, a nesmú od nikoho požadovať ani prijímať pokyny.
3. Člen alebo členovia dozorného orgánu sa zdržia akéhokoľvek konania nezlučiteľného s ich povinnosťami a počas svojho funkčného obdobia nevykonávajú žiadnu inú platenú ani neplatenú pracovnú činnosť nezlučiteľnú s touto funkciou.
4. Každý členský štát zabezpečí, aby sa každému dozornému orgánu poskytli ľudské, technické a finančné zdroje, priestory a infraštruktúra, ktoré sú potrebné na účinné plnenie jeho úloh a vykonávanie jeho právomocí vrátane tých, ktoré sa majú plniť a vykonávať v súvislosti so vzájomnou pomocou, spoluprácou a účasťou vo výbore.
5. Každý členský štát zabezpečí, aby si každý dozorný orgán vybral a mal svoj vlastný personál, ktorý je podriadený výlučne členovi alebo členom dotknutého dozorného orgánu.
6. Každý členský štát zabezpečí, aby každý dozorný orgán podliehal finančnej kontrole, ktorá neovplyvní jeho nezávislosť, a aby mal samostatný verejný ročný rozpočet, ktorý môže byť súčasťou celkového štátneho alebo národného rozpočtu.

Nezávislosť - SDEÚ

- C-518/07, Európska komisia v Spolková republika Nemecko, 9. marca 2010.
- C-614/10, Európska komisia v Rakúska republika, 16. októbra 2012.
- C-288/12, Európska komisia v Maďarsko, 8. apríla 2014.

Čo robí dozorný orgán?



One-Stop-Shop

- koncept „*one-stop shop*“ bol prijatý pre prípady tzv. cezhraničného spracúvania osobných údajov s cieľom určiť na výkon dozoru v rovine praktického vymáhania práva iba jeden (hlavný) dozorný orgán, ktorý bude celý proces dozoru a výkonu opatrení“ vo vzťahu k prevádzkovateľovi prakticky zabezpečovať a v konečnom dôsledku v krajnom prípade aj ako jediný oprávnený subjekt ukladať i sankcie a nápravné opatrenia.
- finálny výsledok normatívneho vyjadrenia princípu jednotného kontaktného miesta v GDPR je zložitý a umožňuje vo viacerých prípadoch vybočenie z tohto pravidla.

One-Stop-Shop

- PODMIENKY:
  - Cezhraničný spracúvanie (čl. 4 bod 23)
  - Existencia hlavnej prevádzkárne alebo
    - Sťažnosť sa týka iba prevádzkárne v konkrétnom členskom štáte
    - Podstatne ovplyvňuje dotknuté osoby iba v konkrétnom členskom štáte

Sankcie

- Článok 83 (Všeobecné podmienky ukladania správnych pokút)
- Článok 84 (Ostatné sankcie)

Sankcie

1. Správne pokuty až do výšky **10 000 000 EUR**, alebo v prípade podniku až **do výšky 2 % celkového svetového ročného obratu** za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia:

a) povinnosti prevádzkovateľa a sprostredkovateľa v súvislosti (i) so spracúvaním údajov dieťaťa na právnom základe súhlasu v službách informačnej spoločnosti, (ii) spracúvania bez identifikácie, (iii) všeobecných povinností prevádzkovateľa alebo sprostredkovateľa, (iv) bezpečnostných opatrení a (v) ustanovení upravujúcich zodpovednú osobu

b) povinnosti certifikačného subjektu

c) povinnosti monitorujúceho subjektu schváleného Kódexu správania

Sankcie

2. Správne pokuty až do výšky **20 000 000 EUR**, alebo v prípade podniku až **do výšky 4 % celkového svetového ročného obratu** za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia:

a) základné zásady spracúvania vrátane podmienok súhlasu;

b) práva dotknutých osôb

c) prenos osobných údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii

d) akékoľvek povinnosti podľa práva členského štátu prijatého na účely osobitných situácii spracúvania

e) nesplnenie príkazu alebo nedodržanie dočasného alebo definitívneho obmedzenia spracúvania alebo pozastavenia tokov údajov nariadeného dozorným orgánom podľa článku 58 ods. 2, alebo v rozpore s článkom 58 ods. 1 neposkytnutie prístupu.

Uložené pokuty svet vs. Slovensko

Entita	Pokuta
Marriott International, Inc *(intent)*	*110,390,200 €*
Google Inc.	*50,000,000 €*
British Airways	20,000,000 €
Austrian Post	18,000,000 €
Sociálna poisťovňa	50.000 €
Slovak Telekom	40.000 €

Sankcie

- Článok 84

1. Členské štáty stanovia pravidlá pre iné sankcie za porušenia tohto nariadenia, predovšetkým za tie, na ktoré sa nevzťahujú správne pokuty podľa článku 83, a prijmú všetky opatrenia potrebné na zabezpečenie ich vykonávania. Takéto sankcie musia byť účinné, primerané a odrádzajúce.

2. Každý členský štát oznámi Komisii do 25. mája 2018 ustanovenia svojich právnych predpisov, ktoré prijme podľa odseku 1, a bezodkladne oznámi aj všetky následné zmeny, ktoré sa týchto ustanovení týkajú.

Napríklad...

§ 374 TZ Neoprávnené nakladanie s osobnými údajmi

(1) Kto neoprávnene poskytne, sprístupní alebo zverejní

a) osobné údaje o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo

b) osobné údaje o inom získané v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie a tým poruší všeobecne záväzným právnym predpisom ustanovenú povinnosť, potrestá sa odňatím slobody až na jeden rok.

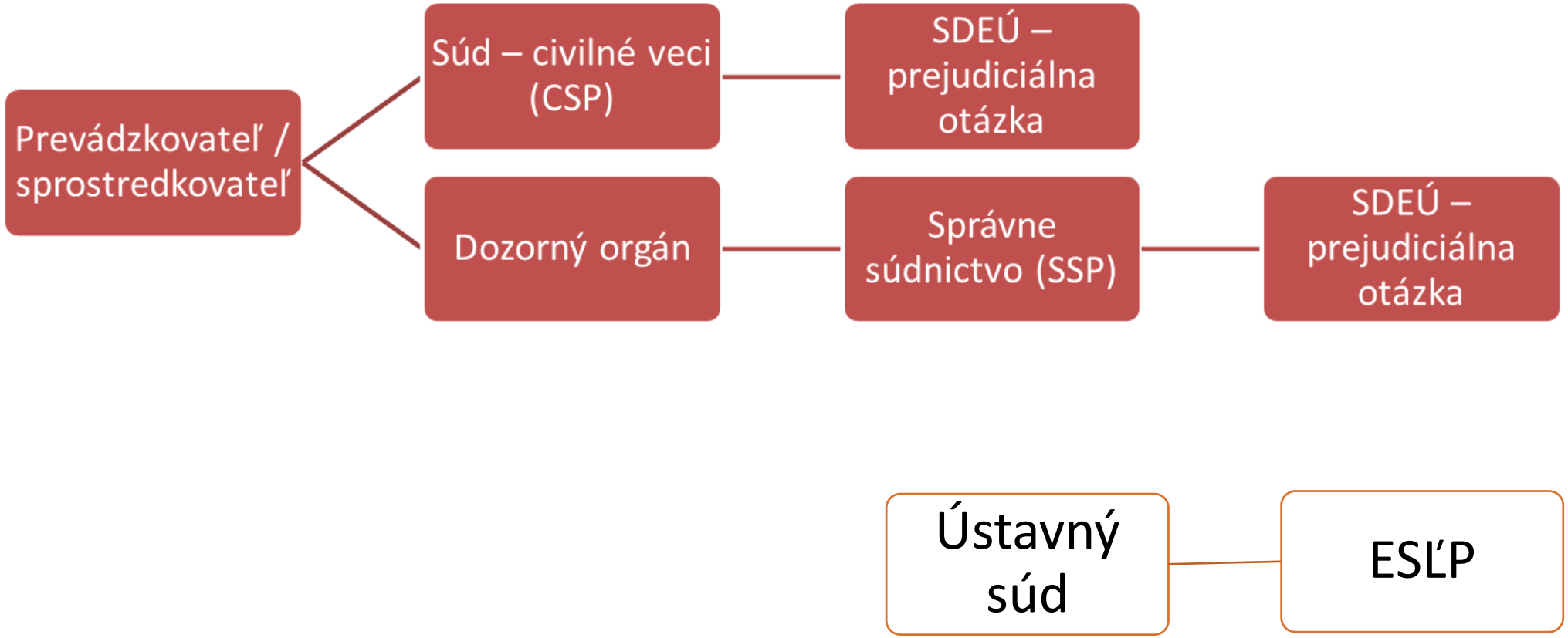
(2) Odňatím slobody až na dva roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) a spôsobí ním vážnu ujmu na právach dotknutej osoby,

b) verejne, alebo

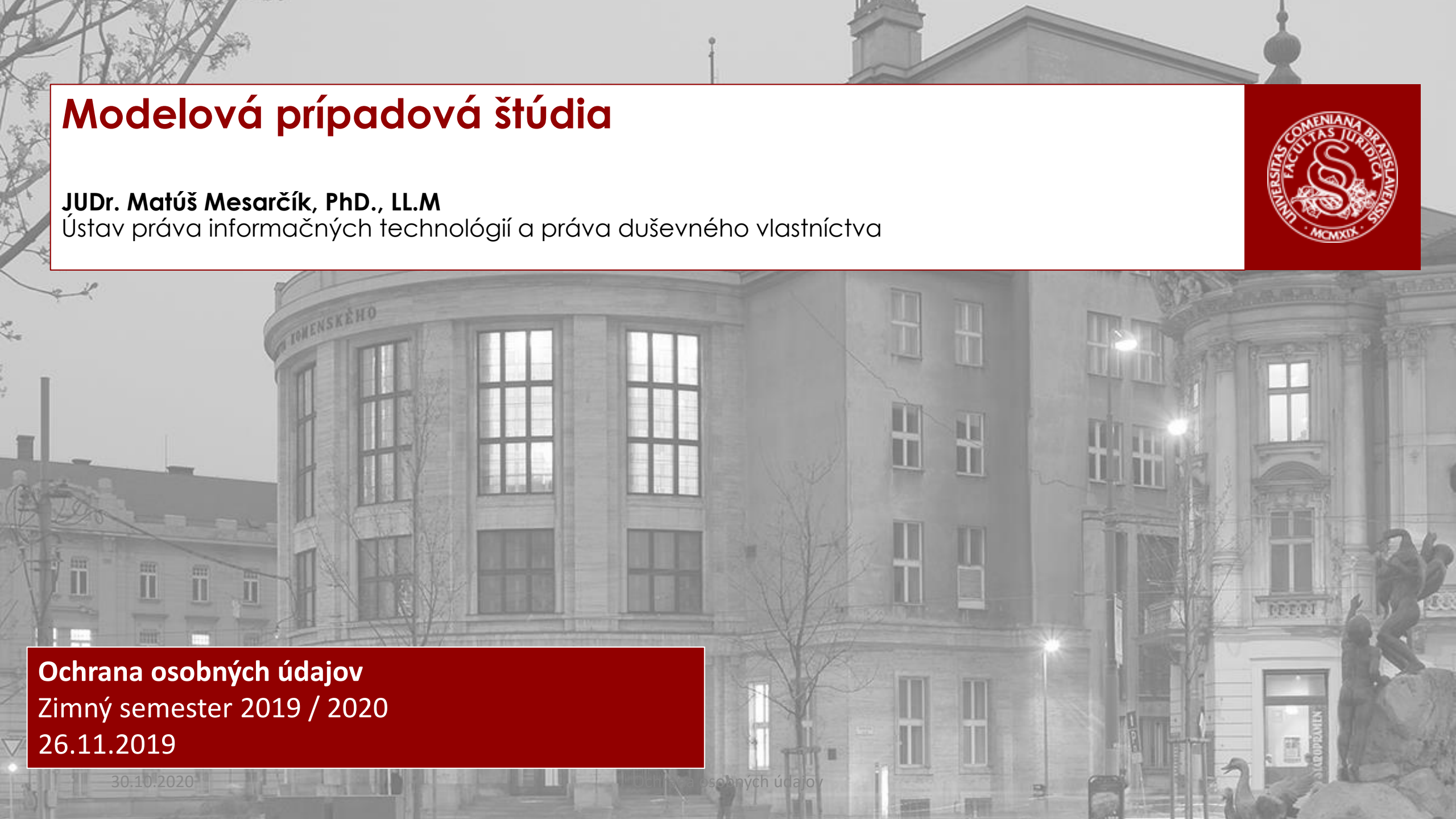
c) závažnejším spôsobom konania.

Prostriedky nápravy



Modelová prípadová štúdia

JUDr. Matúš Mesarčík, PhD., LL.M
Ústav práva informačných technológií a práva duševného vlastníctva



Ochrana osobných údajov
Zimný semester 2019 / 2020
26.11.2019

Prípadová štúdia

Slovenská republika prostredníctvom Úradu pre elektronické služby prevádzkuje portál verejnesluzby.sk, kde môžu občania ale aj iné osoby využívať rôzne služby verejnej správy v elektronickej podobe ako napr. podanie daňového priznania, registrácia a zmena trvalého pobytu alebo založenie živností. Tento webový portál zbiera aj IP adresy návštevníkov (označenie uzla v sieti, z ktorého bolo pristúpené do internetovej siete) za účelom identifikácie páchateľov počítačových potenciálnych trestných činov.

1. **Je IP adresa návštevníkov webového portálu v tejto súvislosti osobným údajom?**
2. **Ako dlho by prevádzkovateľ mohol spracúvať IP adresy návštevníkov portálu za vyššie uvedeným účelom?**
3. **Prevádzkovateľ vymedzil nasledovné účely. Priraďte k ním relevantné právne základy a svoju odpoveď odôvodnite.**
   - **Prevádzka služby (webstránky)**
   - **Personalistika a mzdy**
   - **Daňové a účtovné účely**
   - **Štatistické účely**
   - **Bezpečnosť**
4. **V prípade ak dôjde k bezpečnostnému incidentu a sú kompromitované prihlasovacie údaje občanov do elektronických služieb, ktorej entite (prípadne akým spôsobom) je potrebné takýto bezpečnostný incident nahlásiť?**

Prípadová štúdia

Slovenská republika prostredníctvom Úradu pre elektronické služby prevádzkuje portál verejnesluzby.sk, kde môžu občania ale aj iné osoby využívať rôzne služby verejnej správy v elektronickej podobe ako napr. podanie daňového priznania, registrácia a zmena trvalého pobytu alebo založenie živností. Tento webový portál zbiera aj IP adresy návštevníkov (označenie uzla v sieti, z ktorého bolo pristúpené do internetovej siete) za účelom identifikácie páchateľov počítačových potenciálnych trestných činov.

5. **Prevádzkovateľ sa rozhodne predávať reklamné predmety s logom webstránky verejnesluby.sk (tričká, mikiny, perá, odznaky atď.) a chce zasielať návštevníkom stránky ponuky takýchto tovarov a služieb.**

   a) Za týmto účelom pri registrácii užívateľa vytvorí formulár, v ktorom je možnosť vyjadriť súhlas so zasielaním ponuky tovarov a služieb mailom a v tomto formulári je predvolené zaškrtnuté políčko, ktorým užívateľ vyjadruje súhlas. Je vyjadrenie takéhoto súhlasov v súlade s GDPR?

   b) Bolo by možné podmieniť využívanie portálu verejnesluzby.sk daním súhlasu na zasielanie ponúk tovarov a služieb (bez udelenia súhlasu na marketing by návštevník nemal prístup k elektronickým verejným službám)?

6. **Je Úrad pre elektronické služby povinný poveriť do funkcie zodpovednú osobu?**
7. **Vzhľadom na osobnú pôsobnosť GDPR, v akom postavení je Úrad pre elektronické služby voči:**

   a) Občanom využívajúcim elektronické služby verejnej správy?

   b) Spoločnosti, ktorú poverí vyhotovením analýzy správania užívateľov za účelom vylepšenia webového portálu a služieb?

JUDr. Matúš Mesarčík, PhD., LL.M
Odborný asistent
Ústav práva informačných technológií a práva duševného vlastníctva
Právnická fakulta, Univerzita Komenského v Bratislave
matus.mesarcik@flaw.uniba.sk