

Základy regulácie kybernetickej bezpečnosti a súvisiacich oblastí

Modul 4 - Základy regulácie ochrany súkromia a ochrany
osobných údajov

Časť. 2

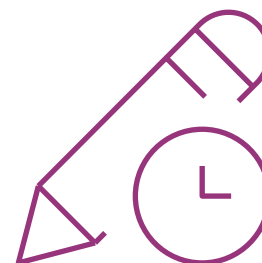
doc. JUDr. Matúš Mesarčík, PhD., LL.M

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



PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-VO1-00002



Agenda

1. Základné zásady spracúvania osobných údajov (2. časť)
2. Manažment práv dotknutých osôb
3. Bezpečnosť pri spracúvaní osobných údajov
4. Zodpovednosť (*accountability*) pri spracúvaní osobných údajov
5. Cezhraničné prenosy osobných údajov
6. Činnosť dozorných orgánov
7. Zodpovednosť a prostriedky nápravy

ZÁKLADNÉ ZÁSADY SPRACÚVANIA

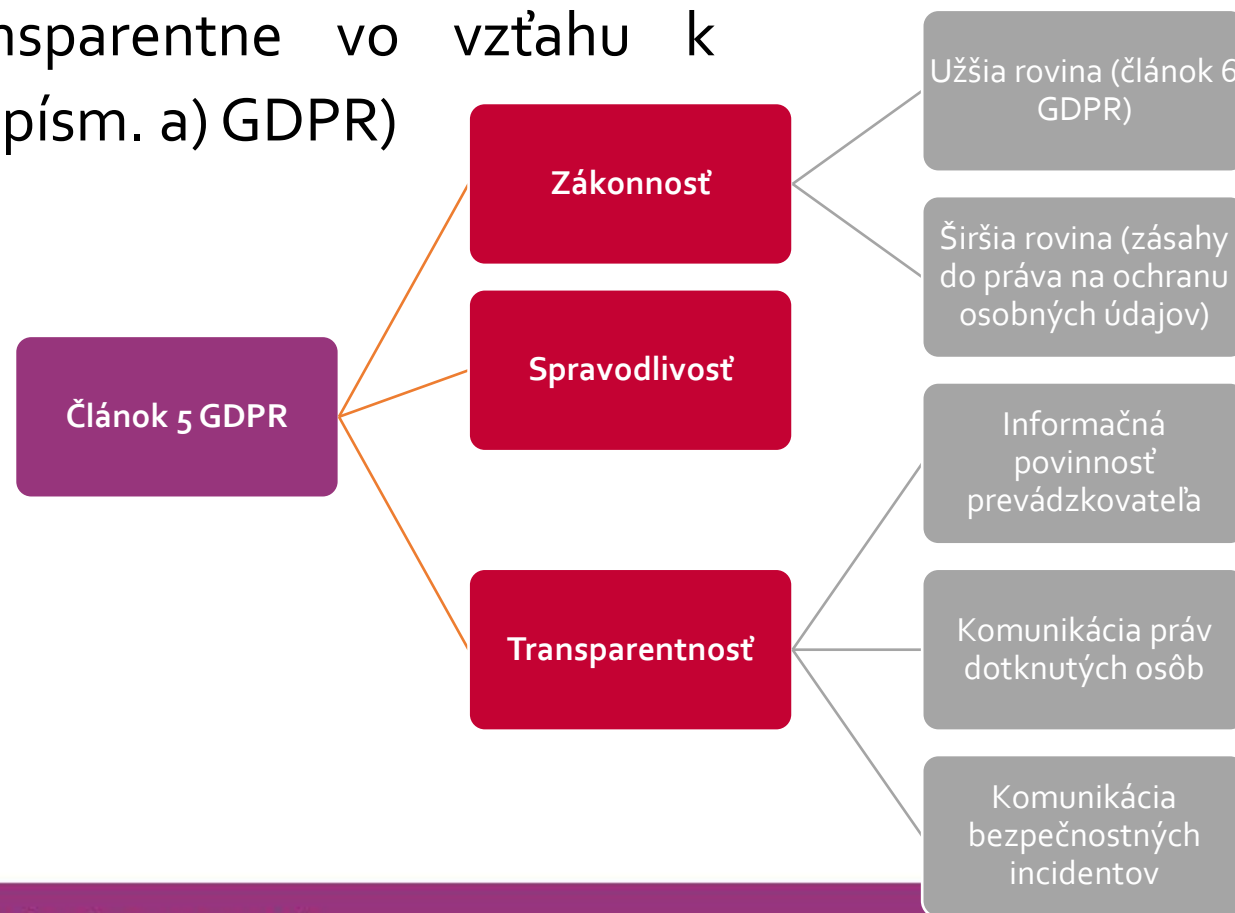
Základné zásady

- **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 uchovávanania (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“ (článok 5 ods. 1 písm. a) GDPR)



Zásada zákonnosti



K.H. a iní proti Slovensku (ESLP)

Zásada spravodlivosti

- Spravodlivosť je všeobecná zásada, ktorá vyžaduje, aby sa osobné údaje nespracúvali spôsobom, ktorý je pre dotknutú osobu neodôvodnene škodlivý, nezákonne diskriminačný, neočakávaný alebo zavádzajúci (EDPB)
- Autonómia
- Interakcia
- Očakávanie
- Nediskriminácia
- Nezneužívanie
- Voľba na spotrebiteľovi
- Rovnováha síl
- Neprenášanie rizika
- Nezavádzanie
- Dodržiavanie práv
- Etika
- Pravdivosť
- Zásah človeka
- Spravodlivé algoritmy

Zásada minimalizácie údajov

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



Zásada správnosti

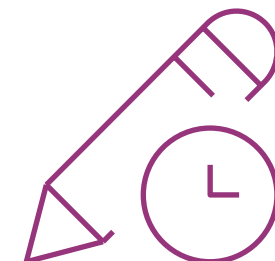
- „Osobné údaje musia byť...správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska **účelov, na ktoré sa spracúvajú**, bezodkladne vymažú alebo opravia“

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

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

- „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)

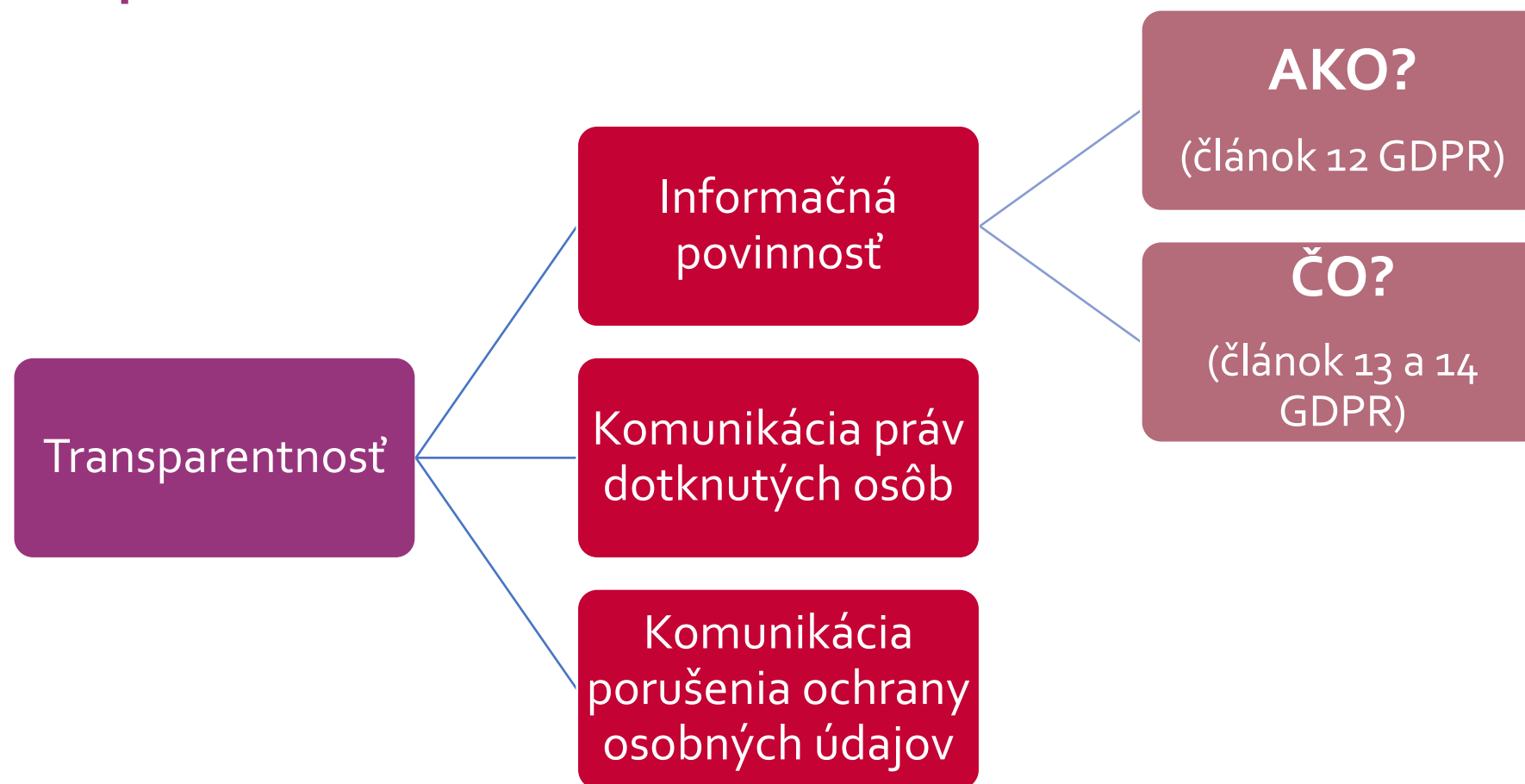
Zásada zodpovednosti - komponenty

- 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)

- 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 uchovávaní 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 Mokrú sa obáva, že táto informácia odhalí údaje o jej sexuálnom živote.

TRANSPARENTNOST (Informačná povinnosť)

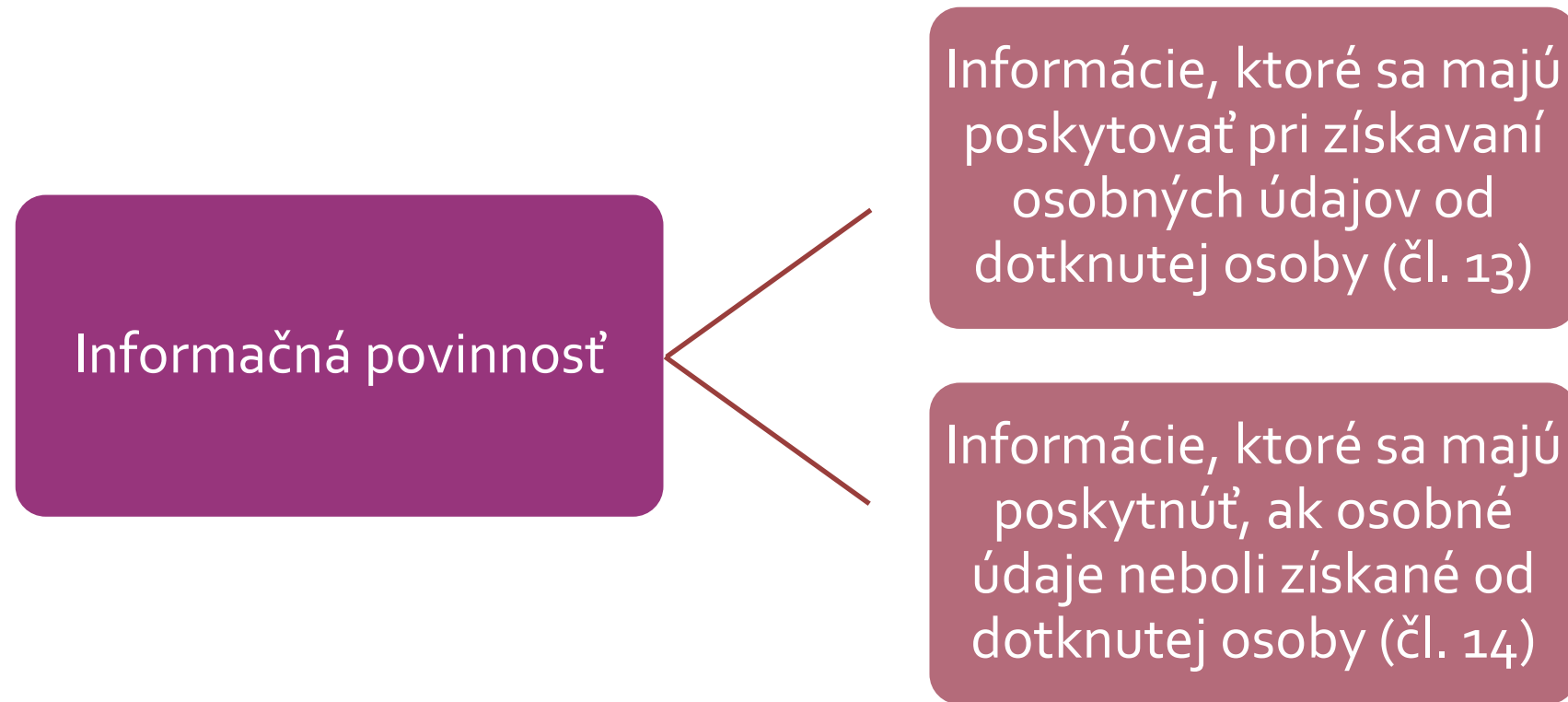
Transparentnosť



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.



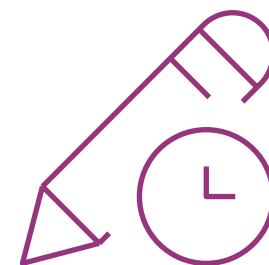
Výnimky z povinnosti

- **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 informácií 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

Úloha

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

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 namietat'	- Právo namietat' (verejný alebo oprávnený záujem) - Právo namietat' voči priamemu marketingu
Právo nebyť predmetom AIR	- Právo na ľudský zásah - Právo vyjadriť stanovisko - Právo napadnúť rozhodnutie

Manažment práv dotknutých osôb

Prijatie žiadosti / Evidencia

Identifikácia dotknutej osoby

Vybavenie žiadosti

**Článok
12 GDPR**

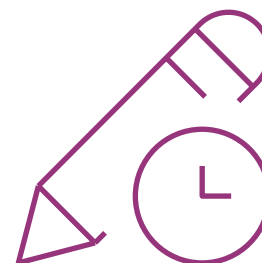
Úloha

OD: veveričiak69@azet.sk

PRE: dpo@superbanka.sk

VEC: Už bolo dosť!

Vy idioti!



Už vás mám dosť! Už stačilo!

Dajte preč tie númerá z mojho účtu inak vás panbožko potrestá!

Novotný

Právo na prístup

- 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.

Právo na vymazanie (článok 17 GDPR)

- „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 aspoň jeden dôvod z článku 17 ods. 1
 - Neaplikuje sa žiadna výnimka z článku 17 ods. 3
- „Zabudnutie v článku 17 ods. 2

Právo na vymazanie (článok 17 GDPR)

- Michal bol vylúčený z internátov UK v Bratislave, pretože niekoľkokrát nedodržiaval protipandemické opatrenia. Interné predpisy UK ustanovujú, že vylúčený, nemôže ďalej žiadať o pridelenie ubytovania. Michal je na toto pravidlo obísť. Podá si žiadosť o vymazanie podľa článku 17 GDPR o vymazanie informácií o jeho vylúčení.
- **Posúďte, či sú splnené podmienky na výkon práva na vymazanie a výnimky?**
- O Michalovom správaní natočí TV Markíza reportáž, ktorá sa našla v archíve. O 15 rokov neskôr, keď je Michal úspešný partner v advokátskej kancelárii, kandidovať na post sudcu Ústavného súdu SR. Nakoľko sa obáva diskreditácie vzhľadom na reportáž, zašle spoločnosti Google žiadosť o vymazanie odkazov na danú reportáž zo všetkých jazykových mutácií vyhľadávača Google.
- **Môže byť Michal pri svojej žiadosti o vymazanie úspešný?**
- **Môže Google vymazať odkazy aj z mimoeurópskych mutácií vyhľadávača?**
- **Vidíte efektívnosť v Michalovom podaní, alebo by ste mu poradili iný postup?**

- **ML and WW v Nemecko (kritéria z Axel Springer)**
 - Miera príspevku do diskusie verejného záujmu
 - Status osoby, ktorej sa prejav týka
 - Predchádzajúce chovanie dotknutej osoby
 - Metóda získania informácie a jej vierohodnosť
 - Obsah, forma a následky zverejnenia informácie

Právo na obmedzenie spracúvania

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

- 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 ak sa spracúvanie vykonáva automatizovanými prostriedkami.

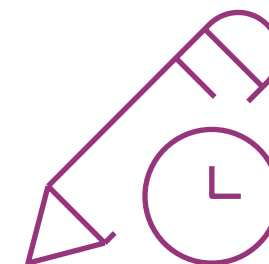
- Na aké údaje sa vzťahuje?
 - Priamo poskytnuté údaje
 - Pozorované údaje
 - Odvodené (agregované) údaje

3 PODMIENKY APLIKÁCIE

1. Typ spracúvania
2. Právny základ
3. Typ údajov
4. Spôsob poskytnutia

Zadanie

- 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 správanie. Údaje o budúcom správaní klienta?



Právo namietat'

- 1. Dotknutá osoba má právo kedykoľvek namietat' 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 namietat' 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 automatizovaného individuálneho rozhodovania

- 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 automatizovaného individuálneho rozhodovania

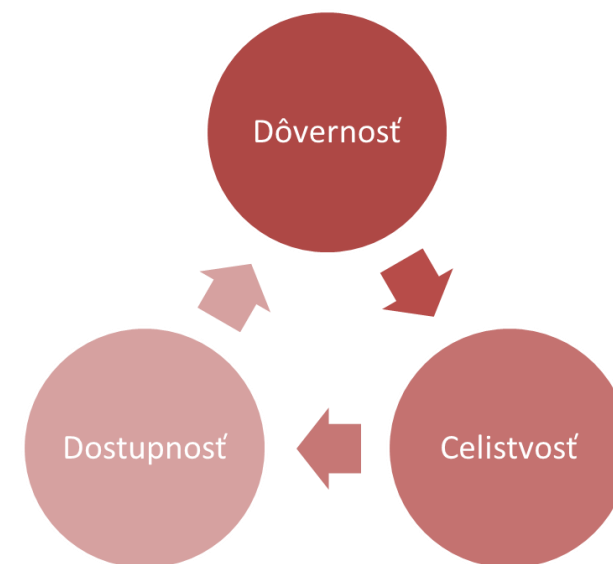
- Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.
- **Prostriedky obrany:**
 - Právo na ľudský zásah
 - Právo vyjadriť stanovisko
 - Právo napadnúť rozhodnutie



Bezpečnosť spracúvania

Bezpečnosť v GDPR

- Zásada dôvernosti a integrity
- Princíp technologickej neutrality
- Štandardizácia (ISO normy) = vzťah s GDPR?
- **GDPR = zohľadňovanie subjektívnych rizík! (Recitál 75)**

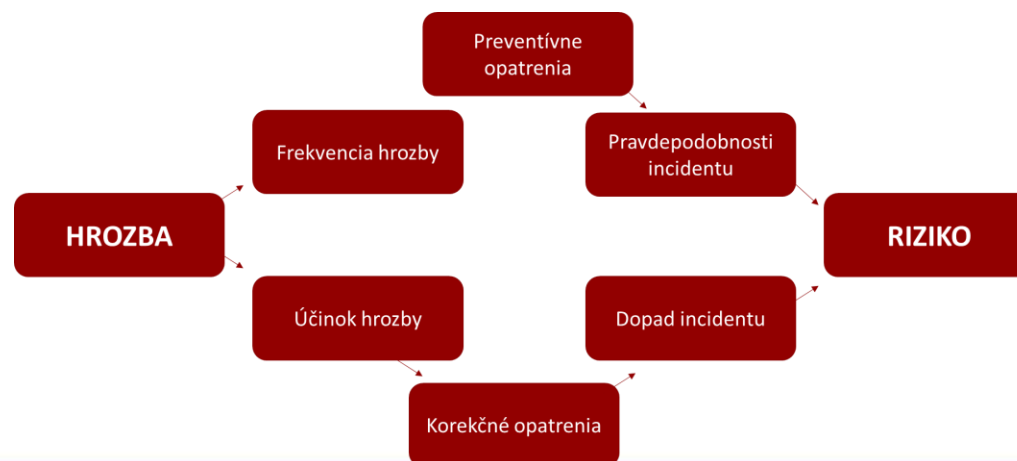


Všeobecná klauzula

Článok 32 (Bezpečnosť spracúvania)

Prevádzkovateľ a sprostredkovateľ prijímú 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.



Technické a organizačné opatrenia

Technické opatrenia	Organizačné opatrenia
Postupy bezpečného obstarávania softwarov	Poučenia poverených osôb
<u>Sieťové</u> firewally	Oddelenie právomocí
Monitorovanie bezpečnosti siete	Pravidlá a kontrola vstupu
Manažment <u>identitít</u>	Vzdelávanie
Šifrovanie alebo <u>pseudonimizácia</u>	Určenie postupov likvidácie údajov
Logovanie	Pravidlá manipulácie s nosičmi
Zálohovanie	Politika čistého stola

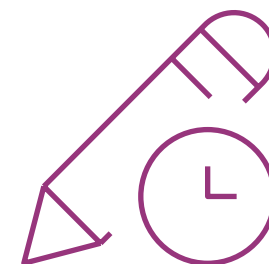
Porušenia ochrany osobných údajov

- 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 (*availability breach*)

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

Nahlasovanie porušenia

- 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 umožňujú 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

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

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 (ods. 1)

2. Všeobecná
klauzula (test rizika)

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. (ods. 3)
- d) ak to určí dozorný orgán

1a. Osobitné prípady

1b. Osobitné prípady
určené dozorným orgánom

Posúdenie vplyvu

- **KRITÉRIA VYSOKÉHO RIZIKA**

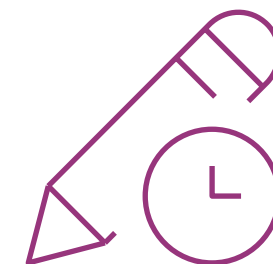
- a) Vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby
- b) Automatizované rozhodovanie s právnym alebo podobne závažným účinkom
- c) Systematické monitorovanie osobných údajov
- d) Spracúvanie citlivých osobných údajov
- e) Spracúvanie údajov vo veľkom rozsahu
- f) Spájanie alebo kombinovanie 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

Posúdenie vplyvu

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 pridelovanie bodov
6. Posúdenie dôveryhodnosti.
7. Posúdenie platobnej schopnosti.
8. Profilovanie
9. Monitoring práce zamestnanca na základe vážnych dôvodov vyplývajúcich z osobitnej povahy činnosti zamestnávateľa
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.

Posúďte potrebu vykonania posúdenia 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 skenovaní 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?



Spôsob vykonania

- 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.

Zodpovedná osoba

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.

Úlohy DPO

Monitorovacia
činnosť

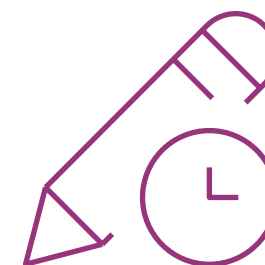
Poradenstvo

Vzdelávanie

Kontaktný bod

Je potrebná 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?
- Telekomunikačný operátor spracúva osobné údaje užívateľov telekomunikačnej siete?
- Výskumná spoločnosť vykonáva testy DNA na vzorke 50 000 ľudí ročne?



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

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, sociálna 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

Modely ochrany osobných údajov

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

Cezhraničné prenosy

- 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?

1. Základné pravidlo

- Základné pravidlo: voľný pohyb osobných údajov po EÚ



2. 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.*“
- Komitológia
- **Posudzované faktory:**
 - Právny štát, dodržiavanie ZLPaSm bezpečnosť, prístup OVM
 - Dozorný orgán
 - Medzinárodné záväzky

Vydané rozhodnutia o primeranosti

- Andorrské kniežatstvo
- Argentína
- Faerské ostrovy
- Guernsey
- Izrael
- Japonsko
- Jersey
- Nový Zéland
- Kanada (komerčné organizácie)
- Ostrov Man
- Švajčiarsko
- Uruguajská východná republika
- Spojené kráľovstvo
- Spojené štáty americké



Júl 2016
Privacy
Shield

Júl 2019
SDEÚ –
Schrems II
(C-311/18)
verejné
vypočutie

**Október
2015**
SDEÚ –
Schrems I
(C-362/14)

Máj 2018
GDPR

Júl 2020
Schrems II – Privacy Shield zrušený!

Júl 2023
EU-US Data Privacy Framework

3. Primerané záruky

- a) **právně závazný a vykonatelný nástroj mezi orgány veřejné 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.
- **SDEÚ vo veci Schrems II: Aj tu je potrebné skúmať úroveň práva tretej krajiny!**

4. Výnimky pre osobitné situácie

- dotknutá osoba vyjadrila **výslovný súhlas** s navrhovaným prenosom po tom, ako bola informovaná o rizikách, ktoré takéto prenosi 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.

4. Výnimky pre osobitné situácie

- 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.
- Obchodná dohoda medzi EÚ a Spojeným kráľovstvom tesne po Brexite (už neplatí)

DOZORNÉ ORGÁNY

ZODPOVEDNOST

SANKCIE

Postavenie dozorných orgánov

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.

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.
- **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

ONE STOP SHOP PROCEDURE

CUSEC

LSA Lead Supervisory Authority

CSAs Concerned Supervisory Authorities

EDPB European Data Protection Board

STEP 1

An individual lodges a complaint or a SA opens a procedure at its own initiative or at the request of another CSA

STEP 3

LSA prepares draft decision and shares with CSAs

STEP 2

LSA carries out inquiry and shares relevant information with CSAs

STEP 4

CSAs provide opinion on the draft decision; LSA takes due account of their views

CSAs have no objections



- LSA adopts decision
- LSA sends decision to controller-processor
- The CSA with which the complaint has been lodged informs the complainant of the decision

LSA follows objections and submits revised draft decision to CSAs

CSAs have reasoned & relevant objections

CSAs have no further objections

CSAs still have objections

LSA does not concur with objections

edpb

European Data Protection Board

Consistency Mechanism kicks in

Case is referred to EDPB for a binding decision



- LSA adopts decision on the basis of EDPB decision
- LSA sends decision to controller-processor
- The CSA with which the complaint has been lodged informs the complainant of the decision

Sankcie (správne pokuty)

- Článok 83 (Všeobecné podmienky ukladania správnych pokút)
- Článok 84 (Ostatné sankcie)
- Správne pokuty
 - Do výšky 10 000 000 eur alebo 2 % z celosvetového obratu (čo je vyššie) Článok 83 ods. 4
 - Do výšky 20 000 000 eur alebo 4 % z celosvetového obratu (čo je vyššie) Článok 83 ods. 5

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.
- **PODMIENKY:**
 - Cezhraničné 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

One-stop-shop

Entita	Pokuta
Meta	1,200,000,000 €
Amazon	746,000,000 €
Meta	405,000,000 €

Entita	Pokuta
Sociálna poisťovňa	50.000 €
Slovak Telekom	40.000 €

Iné sankcie

§ 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 páchatel' 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

