PIKT / Prednáška 9 / 6.5.2013

**13.5.2013** – prednáška nie je, je doskúšanie k zápočtom

**TOTO je posledná prednáška!**

Zákon o osobných údajov sa čoskoro u nás zmení, takže toto všetko môže byť za krátku chvíľu zastarané ☺

# Ochrana osobných údajov

## Medzinárodné pramene (stačí tri vedieť)

* Zmluva o EU v jej medzinárodnom znení
* Európsky dohovor o ochrane ľudských práv
* Smernica Európskeho parlamentu Rady 95/46/EC o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov
* Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov

## Vnútroštátne pramene

* Ústava SR
  + Článok 19
  + Článok 22
* Občiansky zákonník
  + ochrana osobností §11
* Trestný zákon
  + §374
  + §247

## Základné princípy ochrany (toto vraj na skúške nebude, len pre zaujímavosť to máme vedieť ☺)

* Zásada zákonnitosti
* Zásada správnosti
* Zásada určenia účel u spracovania údajov
* Zásada nediskriminácie
* Zásada bezpečnosti
* Dohľad a sankcie
* Cezhraničný prechod osobných údajov

## Predmet zákona

* Ochrana osobných údajov fyzických osôb
* Zásady spracúvania osobných údajov
* Bezpečnosť osobných údajov
* Ochrana práv dotknutých osôb
* Cezhraničný tok osobných údajov
* Registráciu a evidenciu informačných systémov
* Zriadenie, postavenie a pôsobnosť Úradu na ochranu osobných údajov SR

## Pôsobnosť zákona – vzťahuje sa na:

* Orgány štátnej správy
* Orgány územnej samosprávy
* Iné orgány verejnej moci
* Ako aj na právnické a fyzické osoby
  + ktoré spracúvajú osobne údaje
  + určujú účel a prostriedky spracúvania
  + poskytujú osobné údaje na spracovanie
* Na prevádzkovateľov, ktorý nemajú sídlo alebo trvalý pobyt na území SR alebo členského štátu EU
* Osobné údaje, ktoré sú systematicky spracúvané úplne alebo čiastočne spracované automatizovanými prostriedkami

## Nevzťahuje sa na ochranu osobných údajov

* Ktoré spracúva fyzická osoba pre vlastnú potrebu v rámci výlučne osobných alebo domácich údajov, činností ako je vedenie osobného adresára alebo korešpondencia
* Boli získané náhodne bez predchádzajúceho určenia účelu a prostriedkov spracovania, bez zámeru ich ďalšieho spracovania v usporiadanom systéme podľa osobitných kritérií a nie sú ďalej systematicky spracované

## Osobné údaje

* Údaje týkajúceho sa
  + určenie alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo

## Všeobecne použiteľný identifikátor

* Zákon č.. 301/1995 Z.z. o rodnom čísle č. §2

## Osobitbné kategórie osobných údajov

* Rasový alebo etnický pôvod
* Politické názory
* Náboženskú vieru alebo svetonázor
* Členstvo v politických stranách
* Členstvo v odborových organizáciach
* Údaje týkajúce sa zdravia a pohlavného života
* **Zakázané zhromažďovať okrem**
  + ak osoba dala súhlas na takéto zhromažďovanie
  + alebo na základe osobitného zákona
  + ak je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby
  + ak ide o osobné údaje na účel poskytnutia zdravotnej starostlivosti
  + ak ide o spracovanie osobných údajov v sociálnej poisťovni

## Povinné / oprávnené subjekty

* Prevádzkovateľ (FO / PO)
* Sprostredkovateľ (FO / PO)
* Zástupca prevádzkovateľa (FO / PO)
* Zodpovedná osoba (FO)
* Oprávnená osoba (FO)
* Dotknutá osoba (FO)

## Prevádzkovateľ / Zástupca prevádzkovateľa

* Orgán štátnej správy
* Orgán územnej samosprávy
* Orgán verejnej moci
* PO alebo FO, ktorá určuje prostriedky spracovania osobných údajov

## Sprostredkovateľ

* Orgán štátnej správy
* Orgán územnej samosprávy
* Orgán verejnej moci
* PO alebo FO, ktorá spracúva osobné údaje v mene prevádzkovateľa alebo zástupcu prevádzkovateľa

## Zodpovedná osoba

* Fyzická osoba ktorá dozerá na dodržiavanie zákonných ustanovení pri spracovaní osobných údajov
* Ak zamestnávateľ zamestnáva viac ako päť osôb, musí písomne poveriť zodpovednú osobu

## Oprávnená osoba

* Fyzická osoba ktorá prichádza do styku s osobnými údajmi
  + v rámci pracovnoprávneho vzťahu
  + štátnozamestnaneckého pomeru
  + služobného pomeru
  + členského vzťahu
  + na základe poverenia
  + v rámci výkonu verejnej funkcie

## Dotknutá osoba

Každá fyzická osoba ktorej údaje sa spracúvajú.

## Základné povinnosti prevádzkovateľa (§6)

* Pred začatím spracovania jednoznačne vymedziť účel spracovania
* Určiť prostriedky a spôsob spracovania
* Získavať osobné údaje výlučne na vymedzený alebo ustanovený účel
* Aby sa získavali len nevyhnutné osobné údaje, ktoré svojím rozsahom zodpovedajú účelu ich spracovania

## Súhlas dotknutej osoby

* Osobné údaje je možno spracovávať len so súhlasom dotknutej osoby
* Súhlas sa preukazuje zvukovým, zvykovo-obrazovým alebo čestným vyhlásením

## Náležitosti poskytnutého súhlasu

* Kto súhlas poskytol
* Komu sa tento súhlas dáva
* Na aký účel
* Zoznam alebo rozsah osobných údajov
* Dobu platnosti súhlasu
* Podmienky jeho odvolania
* Súhlas daný v písomnej forme je bez vlastnoručného podpisu dotknutej osoby **neplatný**

Osobný údaj sa považuje za správny pokým sa nepreukáže opak

## Likvidácia osobných údajov

* Ak sa splní účel spracovania osobných údajov, prevádzkovateľ bezodkladne zabezpečí ich likvidáciu
* Opravu alebo likvidáciu osobných údajov oznámi prevádzkovateľ do 30 dní od ich vykonania dotknutej osobe a každému komu ich poskytol

Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ a sprostredkovateľ

## Kedy je prevádzkovateľ povinný vypracovať bezpečnostný projekt

* Ak sú v IS spracované osobitné kategórií osobných údajov
* Ak je IS prepojený na verejne dostupnú počítačovú sieť
* Ak je IS prevádzkovaný v počítačovej sieti
* Ak IS slúži na zabezpečenie verejného záujmu

## Ak sa spracúvajú kategórie osobitných údajov

* Právo Úradu na ochranu osobných údajov
  + požadovať od prevádzkovateľa alebo sprostredkovateľa predloženie hodnotiacej správy o výsledku auditu bezpečnosti IS
* Audit bezpečnosti IS
  + môže vykonávať len externá, odborne spôsobilá PO alebo FO
  + ktorá sa nepodieľala na vypracovaní bezpečnostného projektu
  + a nie sú pochybnosti o jej zaujatosti

## Bezpečnostný projekt (§16)

* Vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení
* Spracúva v súlade
  + so základnými pravidlami bezpečnosti
  + vydanými bezpečnostnými štandardmi
  + právnymi predpismi
  + Medzinárodnými zmluvami
* Obsahuje
  + bezpečnostný zámer
  + analýzu bezpečnosti IS
  + bezpečnostné smernice

## Bezpečnostný zámer

* Vymedzuje bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu IS pred ohrozením jeho bezpečnosti

## Analýza bezpečnosti IS

* Je podrobný rozbor stavu bezpečnostného systému
* Obsahuje
  + kvalitatívnu analýzu rizík
  + ...

## Bezpečnostné smernice

* Upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovateľa IS

## Povinnosti zodpovednej osoby (aspoň 4 vedieť)

* Súčinnosť s úradom pri plnení úloh patriacich do jeho pôsobnosti
* Na požiadanie je povinná predložiť kedykoľvek svoje písomné poverenie
* Dohľad nad plnením základných povinností prevádzkovateľa
* Poučenie oprávnených osôb
* Vybavovanie žiadosti dotknutých osôb
* ...

## Úrad na ochranu osobných údajov (aspoň 5 vedieť)

* Ak osobných údajov spracovávajú spravodajské služby, dozor nad ochranou osobných údajov vykonáva Národná rada Slovenskej Republiky podľa osobitného zákona
  + Úrad plní oznamovaciu povinnosť
* Úrad prijíma opatrenia na vykonanie rozhodnutí Európskej komisie vydaných v oblasti ochrany osobných údajov
* Predbežne sleduje stav ochrany osobných údajov, registráciu IS a vedenie evidencie o IS
* Odporúča prevádzkovateľov oparenia na zabezpečenie ochrany osobných údajov v IS
* Kontroluje spracovanie osobných údajov v IS a ukladá sankcie pri porušení povinností uvedených v tomto zákone od prevádzkovateľa a jeho zamestnancov doklady, písomnosti, vyjadrenia, a ďalšie materiály určené na výkon kontroly
  + vrchní inšpektor, ostatní inšpektori, podpredseda úradu, podpredseda úradu sú oprávnení vstupovať na pozemky do budovy alebo miestností prevádzkovateľom a vyžadovať
* Podáva oznámenie orgánom činným v trestnom konaní
* Podieľa sa na príprave všeobecne záväzných právnych predpisov
* Vyjadruje sa k návrhom zákonov
* Predkladá Národnej rade SR správu o stave osobných údajov najmenej raz za dva roky