# ZABEZPEČENIE OSOBNÝCH ÚDAJOV V ORGANIZÁCIÁCH

Peter Filipko – filipko@somi.sk

Daniel Schikor – schikor@somi.sk

# Osobné údaje

Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu – napríklad Meno, priezvisko, akademický titul, dátum narodenia, rodné číslo, adresa, meno, priezvisko, dátum narodenia, rodné číslo, akademický titul, manžela (manželky) a detí počet detí, náboženské vyznanie, majetkové pomery, údaje o dosiahnutom vzdelaní, údaje o príjmoch, poberaní dôchodku, členstvo v politických organizáciách, členstvo v odborovej organizácii... Pritom za jeden z najdôležitejších osobných údajov s atribútom všeobecne použiteľný identifikátor, je považované rodné číslo, ktoré jednoznačne identifikuje dotknutú osobu.

# Osobné údaje

Osobné údaje znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej  alebo identifikovateľnej fyzickej osoby .

- **„akékoľvek informácie“** - Z hľadiska charakteru informácií zahŕňa pojem osobné údaje akýkoľvek druh údajov o osobe. Vzťahuje sa na „objektívne“ informácie a zahŕňa aj „subjektívne“ informácie, názory alebo hodnotenia.

  Príklad : Telefónbanking: V prípade telefónbankingu, pri ktorom sa hlas zákazníka, ktorý dáva banke pokyny, nahráva na pásku, by sa takéto nahrané pokyny mali považovať za osobné údaje.

  Príklad : Videomonitorovanie : Obrazy osôb zachytených systémom videomonitorovania môžu byť osobnými údajmi, pokiaľ sú jednotlivci rozpoznateľní.

# Osobné údaje

- **„týkajúce sa“** - Informácie sa vo všeobecnosti môžu pokladať za informácie, ktoré sa „týkajú“ jednotlivca, ak sú *o uvedenom jednotlivcovi.*

  Tento vzťah sa dá v mnohých situáciách ľahko určiť. Napríklad údaje nachádzajúce sa v individuálnom súbore osoby na personálnom oddelení sa jasne „týkajú“ zamestnaneckého postavenia osoby. Rovnako aj údaje o výsledkoch lekárskych vyšetrení pacienta uvedené v jeho zdravotných záznamoch alebo obraz osoby na videozázname z pohovoru s uvedenou osobou.

  Príklad :  Hodnota konkrétneho domu je informáciou o veci. Je zrejmé, že pravidlá o ochrane údajov sa nebudú uplatňovať v prípadoch, keď sa takáto informácia bude používať iba na uvedenie príkladu úrovne cien nehnuteľností v určitom okrese. Za určitých okolností by sa však takéto informácie mali považovať aj za osobné údaje. Dom je v skutočnosti majetkom vlastníka, ktorý sa takto použije na stanovenie rozsahu povinnosti tejto osoby, napríklad v súvislosti s platením daní. Z tohto hľadiska bude nepopierateľné, že takéto informácie by sa mali pokladať za osobné údaje.

# Osobné údaje

- **„identifikovaná a identifikovateľná“** - Fyzická osoba sa vo všeobecnosti môže považovať za „identifikovanú“ vtedy, keď je v rámci skupiny osôb „odlíšená“ od všetkých ostatných príslušníkov skupiny. Fyzická osoba je preto „identifikovateľná“ vtedy, keď napriek tomu, že osoba ešte nebola identifikovaná, je možné ju identifikovať.

  Osobu možno identifikovať priamo menom alebo nepriamo telefónnym číslom, evidenčným číslom auta, číslom sociálneho poistenia, číslom cestovného pasu alebo spojením dôležitých kritérií, ktoré umožňujú, aby bola spoznaná zúžením skupiny, do ktorej patrí (vek, povolanie, bydlisko, atď.)“.

  Príklad : Zverejnenie röntgenových snímok spolu s pacientovým krstným menom Veľmi nezvyčajná röntgenová snímka jednej ženy bola uverejnená vo vedeckom časopise spolu s jej krstným menom. Krstné meno osoby spolu s vedomosťou jej príbuzných a známych, že trpí určitou chorobou, činia túto osobu identifikovateľnou mnohým osobám a röntgenová snímka by sa potom mala pokladať za osobný údaj.

# Zákon č. 428/2002

- Pojednáva o ochrane osobných údajov.
- Doplnený zákonmi č.602/2003, č. 576/2004, č. 90/2005.
- Zákonom je upravená pôsobnosť, oprávnenia a povinnosti orgánov štátnej správy, územnej samosprávy, verejnej moci ako aj ostatných právnických a fyzických osôb, ktoré spracúvajú a ďalej využívajú osobné údaje.
- Zákon stanovuje, že každý subjekt, ktorý plánuje prevádzkovať informačný systém obsahujúci osobné údaje dotknutých osôb je povinný ešte pred začatím ich spracúvania prihlásiť informačný systém na registráciu, respektíve vykonať nevyhnutné administratívne a procedurálne úkony súvisiace s jeho evidenciou a zosúladením so zákonom.

# Zákon č. 428/2002

- § 6 – pojednáva o povinnostiach prevádzkovateľa – účel a prostriedky spracovania osobných údajov
  - Povinnosť vymedziť účel spracovania osobných údajov pred samotným začatím spracovávania
  - Vylučuje možnosť takých osobných údajov, ktoré sú nezlučiteľné z daným účelom
- § 8 – Osobné kategórie osobných údajov
  - Zakazuje spracovávanie osobných údajov ktoré odhaľujú rasový alebo etnický pôvod, politické názory, vieru, ...
  - Odsek 2 upravuje podmienky spracovávania rodného čísla. rodné číslo možno spracúvať len vtedy, ak bez jeho použitia by mohlo prísť k porušeniu práv a slobôd dotknutých osôb alebo k vážnym chybám pri spracúvaní alebo by bolo znemožnené samotné spracúvanie. Zakazuje sa zverejňovať rodné číslo.

# Zákon č. 428/2002

- § 10 – získavanie osobných údajov
  - Špecifikuje pravidlá získavania osobných údajov do IS
  - Povinnosť informovať dotknutú osobu o účele spracovania osobných údajov a názve a sídle prevádzkovateľa
  - Informovanie o poskytnutí údajov tretej strane
  - Získavanie osobných údajov pri jednorazovom vstupe do priestorov
  - Podmienky monitorovania priestoru videokamerami
- § 13 – likvidácia osobných údajov
  - Po splnení účelu spracovania je potrebné osobné údaje zlikvidovať
  - Upravuje prípady keď sa nevyžaduje bezodkladne likvidácia osobných údajov

# Zákon č. 428/2002

- § 15 – zodpovednosť za bezpečnosť osobných údajov
  - Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ tým, že ich cháni pred náhodným, ako aj nezákonným poškodením a zničením, náhodnou stratou, nedovoleným prístupom a aj akýmikoľvek inými neprípustnými formami spracúvania.
  - Na tento účel prijme primerané technické, organizačné a personálne opatrenia
- § 16 – bezpečnostný projekt
  - Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

# Zákon č. 428/2002

- § 19 – dohľad nad ochranou osobných údajov
  - Za dohľad nad ochranou osobných údajov zodpovedá prevádzkovateľ
  - Ak prevádzkovateľ zamestnáva viac ako päť osôb, výkonom dohľadu poverí zodpovednú osobu. Poverenie musí byť písomné.
  - Povinnosťou prevádzkovateľa je zabezpečiť odborné vyškolenie zodpovedných osôb. Úrad má pravo preveriť vedomosti školeného.
  - Zodpovedná osoba je povinná pred začatím spracúvania osobných údajov vykonať kontrolu, čí ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb.
  - Zodpovedná osoba v priebehu spracúvania osobných údajov upozorňuje na porušenie ustanovení zákona o ochrane osobných údajov

# Zákon č. 428/2002

- §25, § 26 a § 29 – registrácia a evidencia informačného systému
  - Za prihlásenie informačného systému na registráciu zodpovedá prevádzkovateľ. Je povinný ho prihlásiť ešte pred začatím spracúvania osobných údajov.
  - Ak informačný systém podlieha dohľadu zodpovednej osoby, ktorú písomne poveril prevádzkovateľ podľa §19 ods. 2 alebo 8 a ktorá vykonáva dohľad nad ochranou osobných údajov nie je povinný IS registrovať
  - O informačnom systéme, ktorý nepodlieha registrácii, prevádzkovateľ vedie len evidenciu, a to najneskôr odo dňa začatia spracúvania údajov
  - Evidenciu netreba viesť o informačných systémoch ktoré obsahujú osobné údaje slúžiace na identifikáciu osôb pri jednorazovom vstupe do priestorov prevádzkovateľa

# Zodpovedná osoba

- Ak má organizácia viac ako 5 osôb.
- Musí byť písomne poverený zamestnávateľom
- Posudzuje  nebezpečenstvo narušenia osobných údajov
- Zabezpečuje súčinnosť s ÚOOÚ, dohľad nad plnením zákona
- Realizáciu technických, organizačných a personálnych opatrení
- Môže byť len bezúhonná fyzická osoba, nemôže byť štatutár
- Povinnosť informovať ÚOOÚ do 30 dní

# Informačné systémy

- Je to akýkoľvek usporiadaný súbor, sústava, kartotéka alebo databáza obsahujúca osobné údaje o jednej alebo viacerých osobách, ktoré sú systematicky spracúvané s použitím automatizovaných, čiastočne automatizovaných (s použitím programového vybavenia na počítači) alebo iných ako automatizovaných prostriedkov spracúvania (manuálne), napríklad kartotéka, zoznam, register, operát, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia, testy, mzdová agenda, personálna agenda...

- Ak je pripojený do internetu priamo alebo prostredníctvom počítačovej siete je potrebný bezpečnostný projekt

- Ak je určená zodpovedná osoba tak informačný systém stačí len evidovať. Obsahuje údaje podľa § 26 ods. 3

# Bezpečnostný projekt

- Súbor pravidiel, smerníc, opatrení a praktík potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém prevádzkovateľa (spracúvané osobné údaje) z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

- Bezpečnostný projekt tvorí :

  - **Bezpečnostný zámer** – vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému
  - **Analýza bezpečnosti** informačného systému – podrobný rozbor stavu bezpečnosti informačného systému
  - **Bezpečnostné smernice** – upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovateľa informačného systému

# Osobné údaje – elektronická forma

Čo treba mať na zreteli :

- Notebooky a prenosné média – šifrovanie dát
- Mailová a internetová komunikácia – šifrovanie príloh, vírusy, malware
- Prenos dát v lokálnej počítačovej sieti, WiFi
- Zdieľanie dát v počítačovej sieti
- Zabezpečenie dát na počítači
- Archivácia a likvidácia dát

# Osobné údaje – elektronická forma

## Notebooky a prenosné média

- Šifrovanie
- Vynútené šifrovanie a autorizácia zariadení
- Ochrana dát na notebookoch
- Automatické zálohovanie notebookov

# Osobné údaje – elektronická forma

## Mailová a internetová komunikácia

- Šifrovanie mailov
- Vírusy
- Malware
- Sťahovanie súborov na lokálny disk

# Osobné údaje – elektronická forma

## Prenos dát v lokálnej počítačovej sieti

- Bezpečnosť na lokálnej počítačovej sieti
- Zdieľanie údajov
- VPN a šifrovanie
- WiFi a ich zabezpečenie
- Password policy a užívateľské režimy

# Osobné údaje – elektronická forma

## Archivácia a likvidácia dát

- Výhody a nevýhody jednotlivých archivačných médií
- Elektronické skartovačky

# Osobné údaje – papierová forma

Čo je potrebné zabezpečiť :

- Pravidlo čistého stola, dočasné odkladacie boxy na dokumenty
- Diskrétna vzdialenosť a stolové boxy
- Archivácia dokumentov a skartácia dokumentov
- Tlač dokumentov
- Kľúčový režim
- Nepovolané osoby

# Vypracovanie bezpečnostného projektu

# Obsah bezpečnostného projektu

- Bezpečnostný projekt
  - Bezpečnostný zámer
  - Analýza rizík – vymedzenie pojmov
  - Návrh opatrení
  - prílohy
- Bezpečnostná smernica

# Obsah bezpečnostného projektu

Prílohy k bezpečnostnému projektu

- Príloha č.1- Prehľad aktív
- Príloha č.2 - Prehľad hrozieb
- Príloha č.3 - Kategórie správy rizík
- Príloha č.4 - Zoznam strategických osí
- Príloha č.5 - Riziková analýza
- Príloha č.6 - Návrh správy rizík (podľa aktív)
- Príloha č.7 - Návrh správy rizík (podľa hrozieb)
- Príloha č.8 – Návrhy opatrení

# Harmonogram bezpečnostného projektu

**Bezpečnostný projekt harmonogram**

| **Pracovné dni** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dotazník vypracovanie | | | | | | | | | | | | | | | | | | | | | | | | | |
| Uvodné stretnutie | | | | | | | | | | | | | | | | | | | | | | | | | |
| Vypracovanie BP | | | | | | | | | | | | | | | | | | | | | | | | | |
| Konzultácie | | | | | | | | | | | | | | | | | | | | | | | | | |
| Odovzdanie BP, zaškolenie | | | | | | | | | | | | | | | | | | | | | | | | | |

Potrebná súčinnosť pracovníkov : vedúci IT, vedúci personálneho oddelenia, vedúci mzdového oddelenia, vedúci archívu

Vedúci IT - doprovod pri fyzických návštevách pracovísk, konzultácie počas vypracovávania dotazníka

Vedúci personálneho a mzdového - konzultácie

Vedúci archívu - doprovod v priestoroch archívu

# Kde sú informácie

http://www.dataprotection.gov.sk/

http://www.oou.sk/

http://wiki.oou.sk/