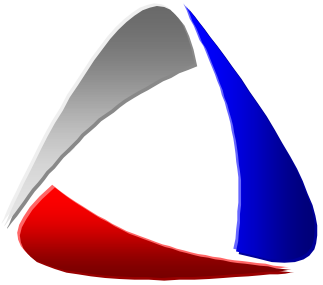
GDPR v prostredí SP



Ing. Juraj Hagara

ITAPA 2018

Legislatívny rámec

- Nariadenie Európskeho parlamentu a Rady EÚ 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR)
- Zákon č. 18/2018 Z.z. o ochrane osobných údajov
- Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy
- Výnos MF SR 55/2014 Z.z. o štandardoch pre IS VS
- Medzinárodné normy pre riadenie bezpečnosti informácií (ISO/IEC 27001, 27002, ISO 27005, 27032)

Interné aktivity 2016

- Detailná mapa aktív SP
- Analýzy rizík
- Analýzy bezpečnostnej a prevádzkovej dokumentácie
- Určenie slabín a hrozieb v ochrane dôležitých aktív SP

Kyberbezpečnostná štúdia 2017

- **Cieľ:**
  Analyzovať a sumarizovať ucelený obraz o stave informačnej bezpečnosti v SP z pohľadu externého poradcu

- **Forma:**
  - analýzy rizík
  - analýzy bezpečnostnej a prevádzkovej dokumentácie SP
  - rozhovory s vlastníkmi údajov, procesov a s kľúčovými hráčmi
  - nasadenie diagnostických sond do interných sieti

- **Výsledok:**
  Štandardné výstupy z analýz vo forme zistení a odporúčaní
  Určené priority, ktoré zohľadnili
  - nesúlad voči platnej legislatíve
  - identifikované riziká a ich mieru
  - systémovosť opatrení
  - časový sled realizácie opatrení

5 jednoduchých otázok

1. aké osobné data občanov EÚ spravujeme
2. ako citlivé data sú to
3. kde sa v rámci SP nachádzajú a kto k nim má prístup
4. ako sa v SP pohybujú, kam a kade z SP odchádzajú
5. ako sa s nimi pracuje a komu sa poskytujú

Nasledujúce aktivity

- Porovnanie výstupov z interných a externých zistení
- Zameranie na:
  - GDPR
  - kyberbezpečnosť
  - IS VS
- Prijaté konkrétne opatrenia na zlepšovanie resp. odstránenie nezhôd
- Vypracovaný časový harmonogram opatrení s predpokladanými finančnými nákladmi na ich realizáciu
- Plnenie opatrení podľa harmonogramu

Povinnosti vyplývajúce z GDPR regulácie

Upresnené práva	Hlásenie incidentov	Zodpovednosti
• Právo na prístup k údajom • Právo na opravu údajov • Právo byť vymazaný • Právo na prenositelnosť	• Schopnost včas objaviť incidenty, analyzovať ich a informovať o nich • Narušenie bezpečnosti dát, musí organizácia nahlásiť do 72 hodín	• Povinnosť primeranosti a povinnosť společnosti minimalizovať objem osobných údajov • Vykonávať analýzu rizík „Posúdenie vplyvu na ochranu osobných údajov“ • Zaistiť a kontrolovať zabezpečenie osobných údajov • Viesť dokumentáciu „Záznamy o činnostiach zpracovania“

Riziká

- Finančné zdroje
  - potreba realizovať aj technické opatrenia

- Verejné obstarávanie
  - riziko nedodržania časového harmonogramu

- Chýba centrálny zastrešujúci orgán pre orgány verejnej moci a verejnej správy
  - NBÚ -> oblasť kyberbezpečnosti
  - Úrad vlády -> oblasť IS VS
  - ÚOOÚ -> GDPR

Otázky a diskusia