GDPR v praxi

Mgr. Ján Cesnak, CISA, CISM, CGEIT, CRISC

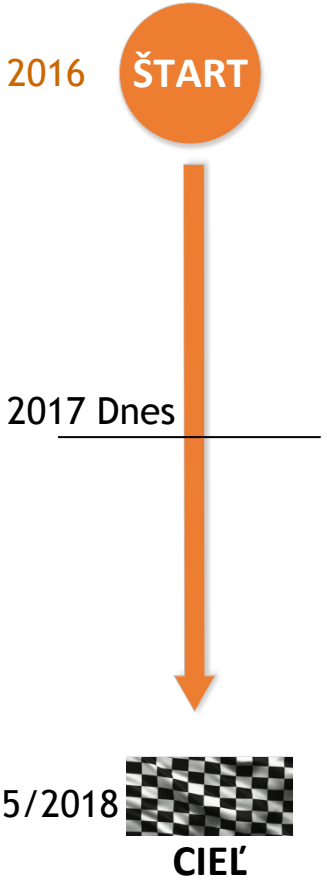
Bratislava 22.6.2017

General Data Protection Regulation

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES je podľa článku 288 Zmluvy o fungovaní Európskej únie všeobecne platný, priamo aplikovateľný právny akt primárneho práva únie, upravujúci pravidlá týkajúce sa ochrany fyzických osôb v súvislosti so spracúvaním osobných údajov a voľného pohybu osobných údajov jednotne pre všetky členské štáty

Nariadenie o ochrane osobných údajov bude účinné a priamo aplikovateľné odo dňa 25. mája 2018

GDPR – čo ďalej



- Preveriť aktuálny stav organizácie – súlad s požiadavkami Nariadenia
- Identifikovať riziká
- Posúdiť vplyv rizík na spracúvané OÚ
- Vypracovať plán čo treba zaktualizovať/zmeniť
- Spracovať dokumentáciu
- Implementovať nové postupy/technológie...
- Zabezpečiť podporu a kontinuitu dohľadu nad ochranou OÚ
- Preškoľovať zamestnancov
- Vylepšovať a kontrolovať
- ...

GDPR – klasický pohľad z praxe

- Viaceré nové požiadavky majú priamy dopad na dostupnosť zdrojov (ľudia, čas, financie)

- Viaceré staršie IS s veľkou pravdepodobnosťou nebudú „kompatibilné“ a ich úprava zrejme ani nebude možná

- Na viaceré aktivity je potrebný outsourcing

- Prax naráža na technologickú nevyspelosť, rôznorodosť, komplikovanosť !!!
- Z praxe -> veľký/viditeľný hráč rieši, zvyšok čaká.

GDPR – klasický pohľad z praxe

Základný problém digitálneho sveta –

- Kópia v digitálnom svete je nerozpoznateľná od originálu – kópia neexistuje, vždy je to originál
- ~~Grafológia, Notár~~


- začína byť záujem o možnosť disponovať spôsobilosťou preukazovania či sa jednalo o moje dáta alebo nie

- je záujem o zadefinovanie „minimalistického štandardu“, ktorý keď bude dodržaný zo strany organizácie, nemali by jej hroziť veľké sankcie
- ***„Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila primeraná bezpečnosť a dôvernosť osobných údajov...“***

GDPR – kyberpriestor a prax

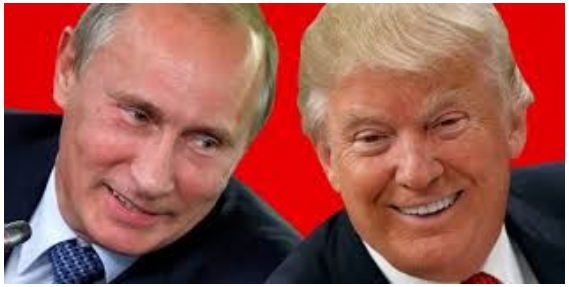
Dáta/OÚ

- sú dnes v cloude,
- vo virtuálnom prostredí
- častokrát geograficky veľmi vzdialené od organizácie
- dokážu prejsť celým svetom za zlomok času
- dokážu byť publikované a následne obratom stiahnuté z webu

Cez globálna sieť bude môcť byť páchaných čoraz väčšie množstvo fraudov – jednorazové aktivity sú prakticky nevystopovateľné -> chýba zdroj.

GDPR – kyberpriestor a prax

- Nárast digitalizácie/elektronizácia a online systémov
- Dve arény s úplne odlišnými praktikami, pravidlami a možnosťami
- Strata hmotného sveta -> presun do cloudu a virtuálneho sveta / kybernetického prostredia, ktoré je bez hraníc
  - ťažké dokazovanie/preukazovanie čo sa stalo, keď je to mimo môjho dosahu
  - priestor na kybernetické útoky/špionáž/sabotáž
  - vzhľadom na vysoké pokuty začne byť tento segment zaujímavým aj pre kyberterorizmus



GDPR

GDPR nie je „one man show“

GDPR nesmie byť len o stavaní plotov

GDPR je kontinuálny živý proces

Ďakujeme za pozornosť

Disig, a. s.
Záhradnícka 151
821 08 Bratislava 2
tel.: 02/ 2085 0140
fax: 02/ 2085 0141
e-mail: disig@disig.sk

www.disig.sk