GDPR nikdy nekončiaci príbeh

... príbeh opradený legendami, mýtusmi, hrôzostrašnými historkami.
Dej plný odvážnych bojovníkov, bájnych rozprávkových bytostí dobrých i zlých,
nádejí i sklamaní, splnených aj nesplnených predsavzatí a sľubov.

vo Vašich kinách od 25.mája 2018 .....už navždy

Jaroslav Oster

…pár myšlienok na úvod

Neformálna diskusia v rámci pracovných debát Asociácie kyberneticej bezpečnosti (AKB):

„Odklonenie zdrojov (pozornosť, čas, financie) od prirodzených problémov (deravá aplikácia, zanedbaná infraštruktúra, poddimenzovaný alebo nedostatočne vzdelaný security staff) ku compliance problému (poďme vyrobiť formálny štít)“

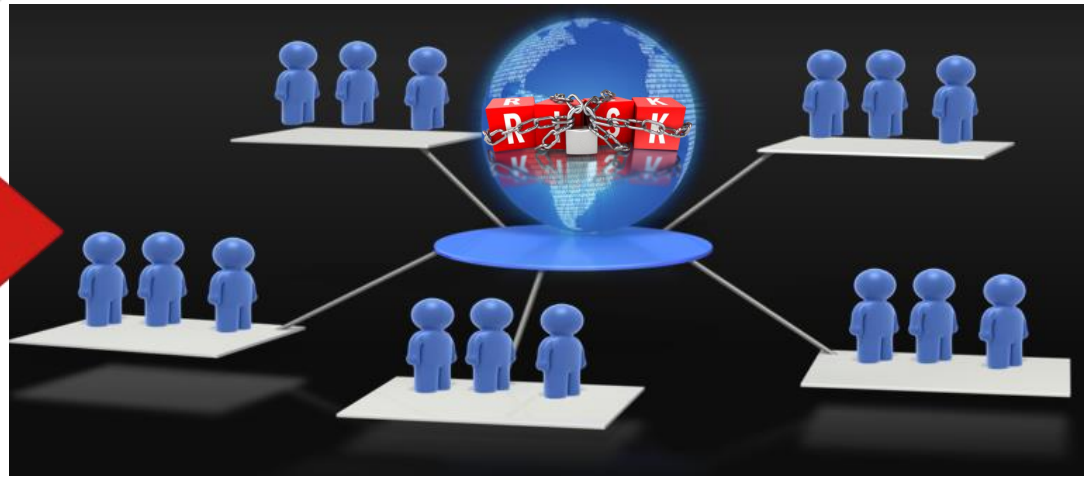
„Prevádzkovatelia si mýlia ochranu prav DO (zmluvy, súhlasy), s reálnou ochranou údajov“

„Totálna nekonzistenia medzi technickými opatreniami na papieri a v praxi“

„Chápanie problematiky v praxi je stále ovplyvňované praktickou implementáciou podľa predošlej legislatívy“

AKB
Asociácia kybernetickej bezpečnosti

GDPR - zámery



Platnosť

27.apríl 2016
oficiálne zverejnenie

Nariadenie Európskeho parlamentu a Rady 2016/679

Analýza

Plán/ Rozpočet

Implementačné procesy

25. máj 2018

GDPR - aktuálny stav v praxi?

GDPR a zákony to vyriešia?

Časté formy úniku

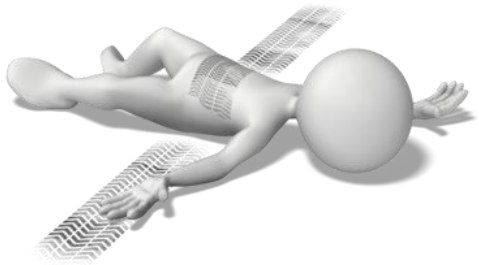
- chyba obsluhy
  - neznalosť, arogancia, cielené obchádzanie opatrení
  - necvičený personál
  - zámerné konanie
- organizačné nedostatky/problémy riadenia
- nezabezpečený prevádzkový perimeter na všetkých úrovniach
- chyby IS
  - chyby vývoja IS – funkčné chyby
  - zlé konfigurácie OS/ SW
- a široký rad ďalších frekventovaných chýb

Mýtus: Máme špičkové IT oddelenie

Technické opatrenia vyriešia všetko

„my máme nasadené špičkové bezpečnostné riešenia, všetko je vyriešené, naši ľudia sú uvedomelí“

- technické riešenie pokrýva obvykle konkrétne riziko/ skupinu rizík
- nerieši organizačné problémy
- nerieši otázky bezpečnostného **povedomia** používateľov IS a už vôbec nie koncepčného a efektívneho vzdelávania

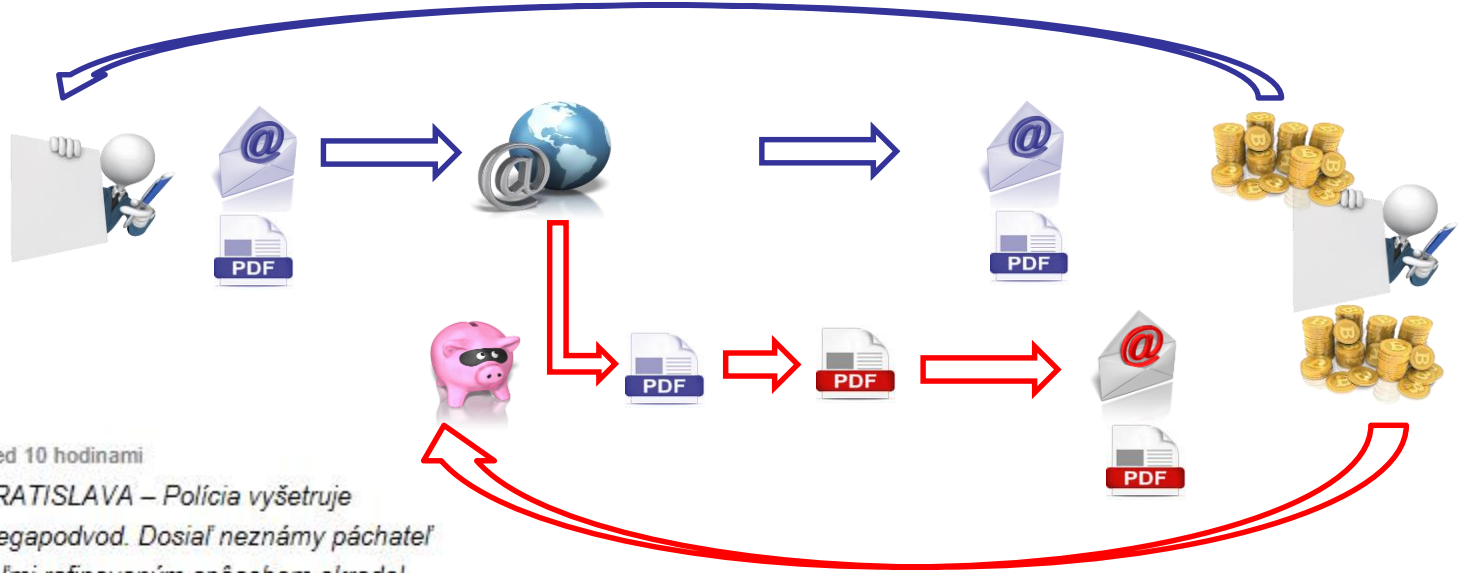


môžeme snáď predpokladať, že autonómne autá dáme do rúk (ne)vodičom bez vodičského oprávnenia?

A je to tu zas ... manipulačné techniky v realite

Podvody s faktúrou....len trochu upravené

2016-2017.....2018



Ilustračné foto
Zdroj: Getty Images

pred 10 hodinami

BRATISLAVA – Polícia vyšetruje megapodvod. Dosiaľ neznámy páchateľ veľmi rafinovaným spôsobom okradol spoločnosť o 167 524 eur. Muži zákona i Ministerstvo vnútra SR (MV SR) v tejto súvislosti upozorňujú verejnosť na podvodné prevody peňazí. Poškodená firma prišla o danú sumu len jedným kliknutím.

LUDSKY FAKTOR

Okrúhly stôl – DIGITÁLNE ZDRAVOTNÍCTVO BEZPEČNE

Dominantný záver:

„Bez vzdelávania na všetkých úrovniach to nepôjde. Vzdelanosť a povedomie je pre kybernetickú bezpečnosť rizikovým faktorom číslo jeden.“

Lukáš Hlavička, riaditeľ vládnej jednotky CSIRT pri ÚPVII

„zabezpečenie dostatočného vzdelanie svojich pracovníkov má byť prioritou pre každého zamestnávateľa, vrátane štátu.“

Rastislav Janota, NBÚ

„Elektronické zdravotníctvo je užitočná vec, ale nemožno ho implementovať bez zohľadnenia ľudského faktora,“

MUDr. Jana Bendová, hlavná odborníčka pre všeobecné lekárstvo, SSVPL

Zabudnite na „poučenie“

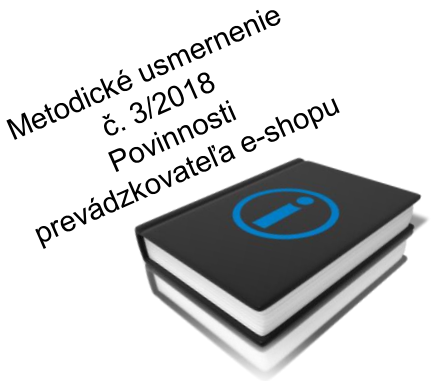
Mýtus: SW support?

Ak nie je náš tak je sprostredkovateľ

4.3 Technická podpora poskytovaná prevádzkovateľovi e-shopu tretím subjektom

Ak tretia strana zabezpečuje pre e-shop technickú podporu, kedy pri odstraňovaní technických problémov môže tento subjekt, resp. jeho zamestnanci vidieť osobné údaje zákazníkov e-shopu a nedochádza zo strany subjektu vykonávajúceho technickú podporu k ďalšiemu spracúvaniu osobných údajov (t. j. osobné údaje napr. len „vidí“, ale ďalej ich nespracúva) postačuje, ***aby bola v zmluve medzi prevádzkovateľom a poskytovateľom technickej podpory ustanovená povinnosť zachovávať mlčanlivosť a prijať primerané bezpečnostné opatrenia (organizačné a technické). Uvedené platí aj vo vzťahu k vykonávaniu technickej podpory prostredníctvom vzdialeného prístupu****.*

- zvažujte aj pohľad z hľadiska rizikovosti



Mýtus: Súhlasy

Súhlasy, súhlasy, súhlasy, oprávený záujem a iné dôvody

v praxi vyžadované súhlasy často nezmyselne v duchu „pre istotu“

- častý **rozpor** (súbeh) s inými právnymi základmi
- **vynucovaný** súhlas
  - platný súhlas musí byť: **dobrovoľný**, preukazný a odvolateľný
  - súhlas pre spracovanie OÚ v pracovno-právnom vzťahu **nie je** dobrovoľný
- oprávnený záujem prevádzkovateľa
  - často zlá aplikácia
  - chýba test proporcionality

ÚSKALIE SÚHLASU

- dotknutou osobou kedykoľvek odvolateľný
- čo potom?

Chaos v súhlasoch

Spracovanie osobných údajov je neprípustné – GDPR definuje výnimky:

- dotknutá osoba **vyjadrila súhlas** so spracúvaním OÚ na jeden alebo viaceré konkrétne účely
- spracúvanie je nevyhnutné **pre plnenie zmluvy**, ktorej zmluvnou stranou je dotknutá osoba
- spracúvanie je nevyhnutné **pre splnenie zákonnej povinnosti** prevádzkovateľa
- spracovanie je nevyhnutné na účel **oprávneného záujmu** prevádzkovateľa
- spracúvanie je nevyhnutné, aby sa ochránili **životne dôležité záujmy** dotknutej osoby alebo inej fyzickej osoby
- spracúvanie je nevyhnutné na splnenie úlohy realizovanej **vo verejnom záujme** alebo pri **výkone verejnej moci** zverenej prevádzkovateľovi

Mýtus: Dodanie na kľúč

Dodávateľ aplikačného IS to vyrieši „na kľúč“

čo môže vyriešiť

- bezpečnosť na svojej aplikačnej úrovni
- efektivizáciu, automatizáciu procesov plnenia povinností prevádzkovateľa vo vzťahu k právam DO
  - informačná povinnost voči DO
  - efektívny prístup k OÚ pri žiadosti DO o poskytnutie infomácie, prenositeľnosť, obmedzenie spracovania, opravu, zabudnutie a ďalšie

Dokumentáciu máme kúpenú ako univerzálny balík

- krabicové riešenia môže byť polotovarom,
- terminologický chaos

  preberanie dokumentácie z českého prostredia

  „**Správce**“ = „**Správca**“ ale u nás „**Prevádzkovateľ**“
- „tvorcovia“ dokumentácie si zaviedli často vlastné terminologické pojmy
- GDPR kladie dôraz na reálnu **implementáciu** opatrení

Mýtus: GDPR versus normy

GDPR nie je/je ISO27xxx

čiastočná pravda, zavedenie procesov podla ISO27xxx nerieši celé spektrum tém GDPR

- GDPR základnou filozofiou smeruje k riadeniu rizík
- riadenie rizík bez vhodnej metodiky je riziko samo o sebe

Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky 158/2018 Z.z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

Príloha k vyhláške č. 158/2018 Z. z.

OPATRENIE NA ELIMINÁCIU RIZÍK PRE PRÁVA FYZICKEJ OSOBY

1. Technické opatrenia

1.1 Technické opatrenie realizované prostriedkami fyzickej povahy

1.1.1 Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).

1.1.2 Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, mreže alebo presklenia).

1.1.3 Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.

1.1.4 Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.

1.1.5 Opatrenie na zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).

Mýtus: Zodpovedná osoba

DPO je chránený živočích

„zodpovednej osobe nemôžete dať výpoveď“

GDPR, oddiel 4, článok 38 recitál 3: Postavenie zodpovednej osoby
.....Prevádzkovateľ ani sprostredkovateľ ju nesmú odvolať za výkon jej úloh...

DPO zamestnanec
zákonník práce/ zákon o štátnej službe
- porušenie pracovnej disciplíny
- neplnenie pracovných povinností
- spôsobenie škody

DPO externý dodávateľ služby
obchodný zákonník
- zmluvné podmienky
- zodpovednosť za škody spôsobené nekvalitným a nie včasným dodávaním služby

Mýtus: Nič sa nedeje

10/2018, ČR
MALL.CZ
pokuta 1,5 mil. Kč
únik nezabezpečených dát zákazníkov

10/2018 ČR/Poľsko
www.znamylekar.cz
dozorový úrad Poľsko preberá kauzu
na základe podania českých lekárov

9/2018 ČR
www.centralniregistrdluzniku.cz.
neoprávnené nakladanie s osobnými
údajmi

7/2018, Francúzsko
vyšetrovanie vo veci FIDZUP/TEEMO
zasielanie reklamy na základe geolokačných dát


Ilustračné foto
Zdroj: Getty Images

pred 10 hodinami

BRATISLAVA – Polícia vyšetruje megapodvod. Dosiaľ neznámy páchateľ veľmi rafinovaným spôsobom okradol spoločnosť o 167 524 eur. Muži zákona i Ministerstvo vnútra SR (MV SR) v tejto súvislosti upozorňujú verejnosť na podvodné prevody peňazí. Poškodená firma prišla o danú sumu len jedným kliknutím.

...instantné, bezpracné a finálne riešenie neexistuje, zmierte sa s tým

Jaro Oster

Info consult, s.r.o.
Martina Rázusa 29
Lučenec

0905 272066

www.infoconsult.sk

oster infoconsult.sk