

Možnosti identifikácie spracovateľských operácií a ich riziková analýza

Marek Zeman, Tatra banka



Čo by mala obsahovať DPIA?

- Východiská
 - Identifikovanie potreby robiť PIA
 - Popis procesu a data flow
 - Normy pre spracovanie
 - Zoznam skratiek a pojmov
- Spracovanie osobných údajov
 - Zásady spracúvania
 - Účel spracúvania
 - Návrh prístupu k analýze
- Identifikácia informačných aktív
 - Zoznam spracovateľských operácií
 - Analýza súladu dokumentácie voči GDPR
 - Bezpečnostná architektúra
 - Bezpečnostné opatrenia
- Analýza rizík
 - Metodika
 - Rozhodnutie o vykonaní posúdenia vplyvu
 - Identifikácia IT rizík a rizík os. Úd.
 - Zraniteľností
 - Hrozieb
 - Rizík
 - Dopadov rizík
 - Ošetrenie rizika
 - Zvyškové riziko
 - Výsledok analýzy za proces
 - Zoznam odporúčaní

Požiadavky na analýzu rizík

Staré – zakomponovať IT Risk assesment

Pozrieť sa na riziká z pohľadu klienta



Identifikovať operácie/procesy vhodné pre DPIA



Strihanie problému

Delenie

- Vzhľadom na operácie
 - málo operácií, každá má veľa atribútov
- Vzhľadom na firemné procesy
 - veľa procesov, otázka je ako urobiť prioritu
- Vzhľadom na IT procesy
 - Bottom – up
- Nevyhnutné – vyplývajú priamo zo zákona

Cesta cez firemné procesy

- V čom je základ
 - IT Risk analýza sa robí od zoznamu procesov a pohľadu biznis vlastníka, až po jednotlivé počítače a komunikáciu
- Čo máme
 - Máme zoznam procesov
 - Biznisovú prioritizáciu
- Čo potrebujeme
 - Treba zabezpečiť analýzu rizík vzhľadom na osobné údaje.
 - Skontrolovať, či je IT Risk analýza kompletná.
 - Rozhodnúť na základe Risk assesmentu pre OU, pre ktoré procesy vytvoriť DPIA

Cesta vzhľadom na IT procesy

- Predpoklady
 - Máme popísané
 - Systémy (kde sú aké údaje a ich spracovávanie).
 - Procesy nad nimi od začiatku až po koniec.
 - Vieme kde máme všetky osobné údaje uložené
 - Je urobený IT Risk assesment na všetky dielčie systémy a komunikáciu.
- Čo urobiť
 - Na základe máp k EA je potrebné identifikovať spracovateľské operácie vzhľadom na IT svet.
 - Urobiť Risk assesment pre osobné dáta
 - Skontrolovať úplnosť IT Risk assesmentu
 - Rozhodnúť sa, pre ktoré IT procesy robiť DPIA

Ako robíť IT Risk assessment?

Identify

- Impact areas
- IT Assets (1-6, + 1+n)
- Threat Agents
- Threat motivation
- Agents capacity and motivation
- Threat agents value (relation: motivation and capacity per threat)
- Vulnerabilities
- Vulnerability Assessment Value = (relation Exposure,Severity)
- Identify IT Risks (through IT Risk Assessment)

Ako robíť Privacy Risk assessment

Source

- ENISA
- LINDDUN
- STRIDE
- ISO

Identify

- Data privacy Goals

Linking

- Data Privacy Goals and relevant LINDDUN and STRIDE Threats
- Privacy Threats (PT) to Threats TBG Threat Catalogue



Ďakujem za pozornosť

Marek Zeman, Tatra banka

