

Nariadenie o ochrane osobných údajov

Nový systém bezpečnostných opatrení

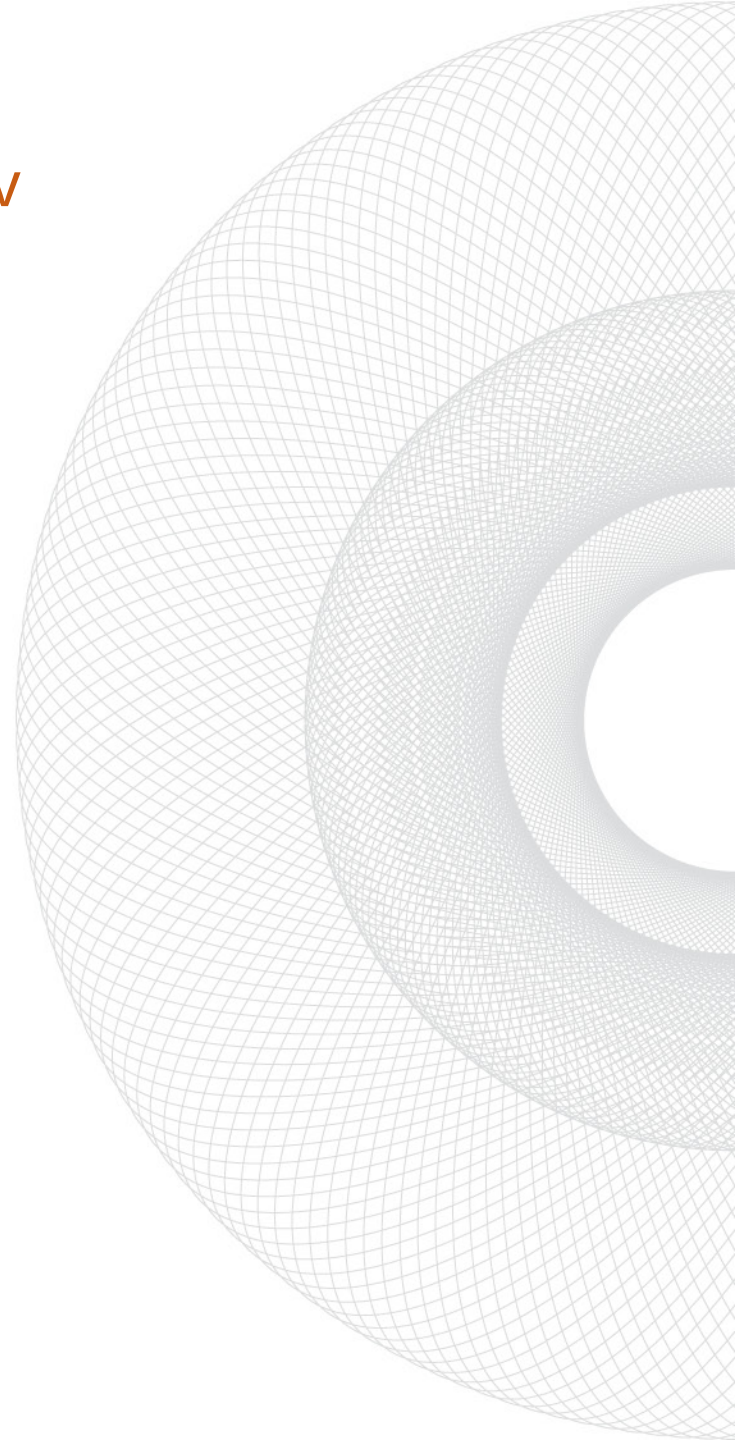
KINSTELLAR

Jakub Berthoty LL.M

Associate

Advokát

Bratislava, 29. september 2016



Úvod a obsah

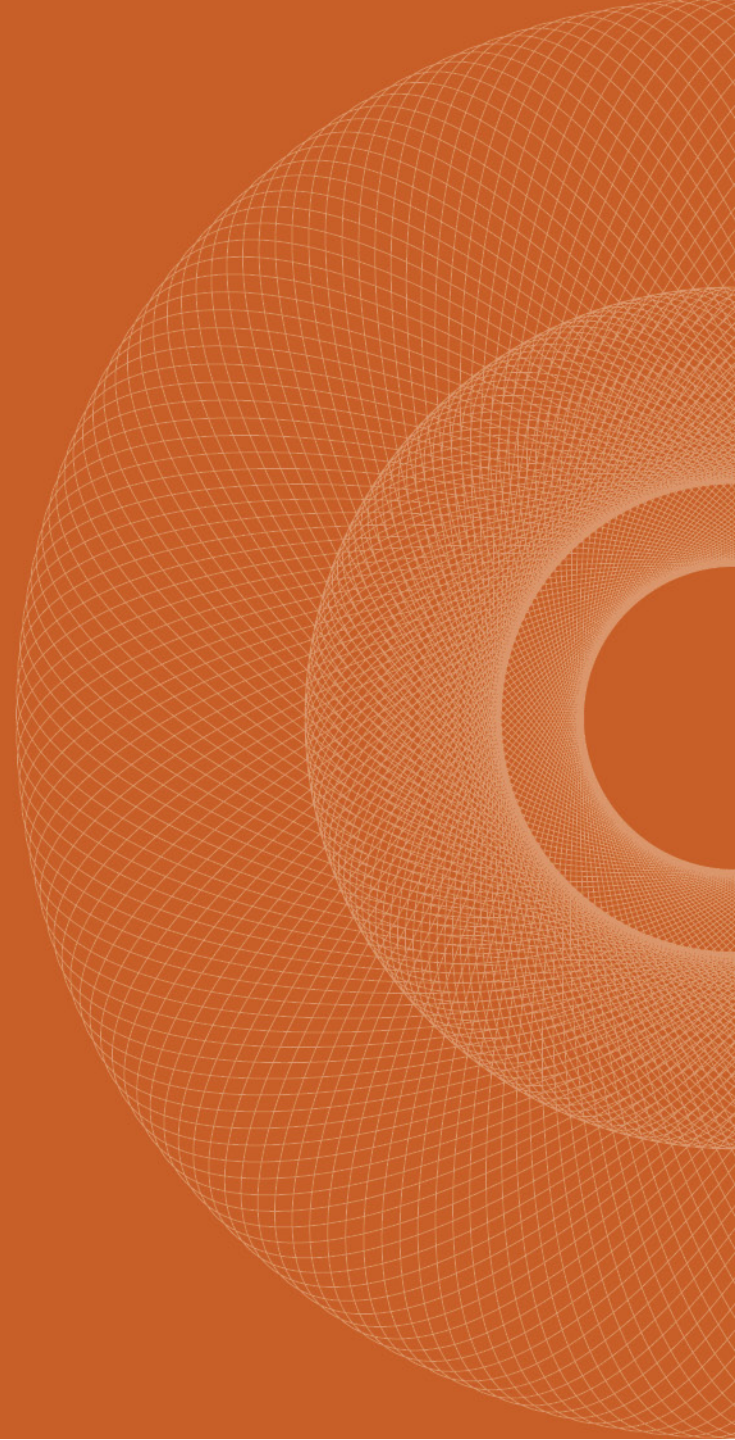
- Prečo bezpečnostné opatrenia?
- Prečo dôraz na IT infraštruktúru a softvér?

Obsah:

- Terajšia úprava
- Nová úprava podľa Nariadenia
- Porovnanie zmien
- Niektoré ďalšie zmeny
- Kde začať?



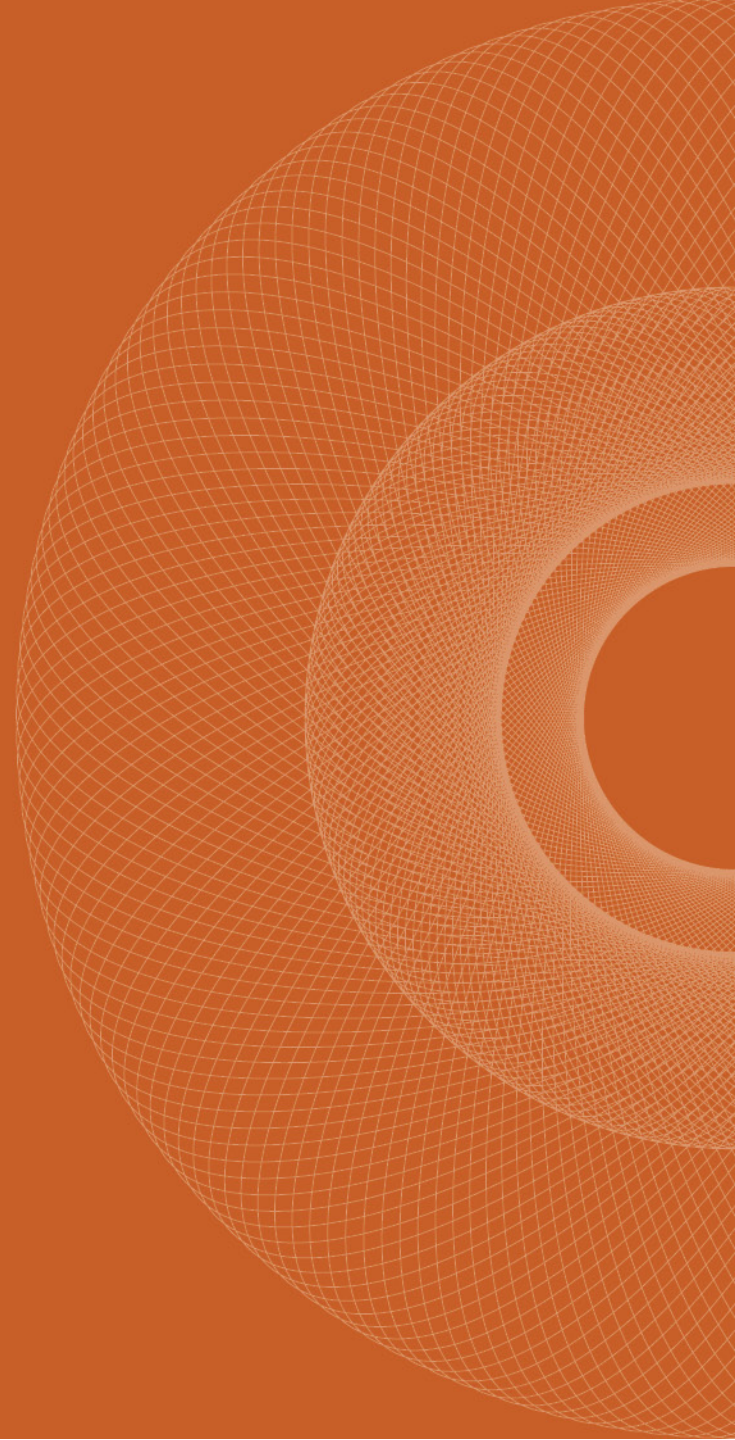
Terajšia úprava



Terajšia úprava bezpečnostných opatrení

- **Bezpečnostné opatrenia podľa zákona č. 122/2013 Z.z.:**
 - prevádzkovateľ je povinný prijať primerané bezpečnostné opatrenia, ktoré zodpovedajú spôsobu spracúvania osobných údajov; berúc do úvahy použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných údajov ako aj rozsah možných rizík spôsobilých narušiť bezpečnosť alebo funkčnosť informačného systému;
 - a zároveň zabezpečiť aktualizáciu bezpečnostných opatrení ak nastali zmeny pri spracúvaní osobných údajov.
- **Vyhláška č. 164/2013 obsahuje zoznam konkrétnych bezpečnostných opatrení**
 - Pri prijímaní a dokumentovaní bezpečnostných opatrení sa primerane použijú najmä bezpečnostné opatrenia uvedené v prílohe:
 - Šifrovanie, antivírus, antispam, firewall, ochrana proti hackerským útokom, pravidelné zálohovanie, legálny softvér, riadenie prístupu, identifikácia používateľov, bezpečná likvidácia a pod.;

Nariadenie



Nový systém bezpečnostných opatrení

- Nariadenie obsahuje požiadavky:
 - na bezpečnosť spracúvania údajov (všeobecné);
 - štandardnej ochrany osobných údajov (*data protection by default*); a
 - špecificky navrhutej ochrana osobných údajov (*data protection by design*).
- Zmeny v bezpečnostných opatreniach je potrebné dokončiť najneskôr do 25. mája 2018.



Bezpečnosť spracúvania údajov – čl. 32

- Ide o všeobecné požiadavky na bezpečnosť údajov.
- Prevádzkovateľ a sprostredkovateľ sú povinní so zreteľom na najnovšie poznatky ('state of the art') berúc do úvahy náklady na ich implementáciu opatrení, implementovať primerané bezpečnostné opatrenia, ktoré zahŕňajú aj:
 - Presudonymizáciu;
 - šifrovanie;
 - Schopnosti zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb (antivírus, firewall, antispam, atď.);
 - Schopnosti včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu (zálohovanie, data recovery);
 - Proces pravidelného testovania, posudzovania a hodnotenia účinnosti bezpečnostných opatrení (penetration testing?).
- Je potrebné zohľadniť aj riziká s rôznou pravdepodobnosťou a závažnosťou pre práva

Štandardná ochrana osobných údajov – čl. 25 (2)

- V podstate ide o minimálne bezpečnostné požiadavky, ktoré platia bez ohľadu na okolnosti vždy.
- Štandardná ochrana osobných údajov (*data protection by default*) znamená, že prevádzkovateľ musí (štandardne) implementovať také bezpečnostné opatrenia, ktoré zabezpečujú, že sa spracúvajú len osobné údaje nevyhnutné pre účely spracúvania, pričom táto podmienka nevyhnutnosti sa rovnako vzťahuje aj na:
 - Množstvo získaných osobných údajov;
 - Rozsah spracúvania osobných údajov;
 - Dobu uchovávania; a
 - Ich prístupnosť/dostupnosť.
- Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

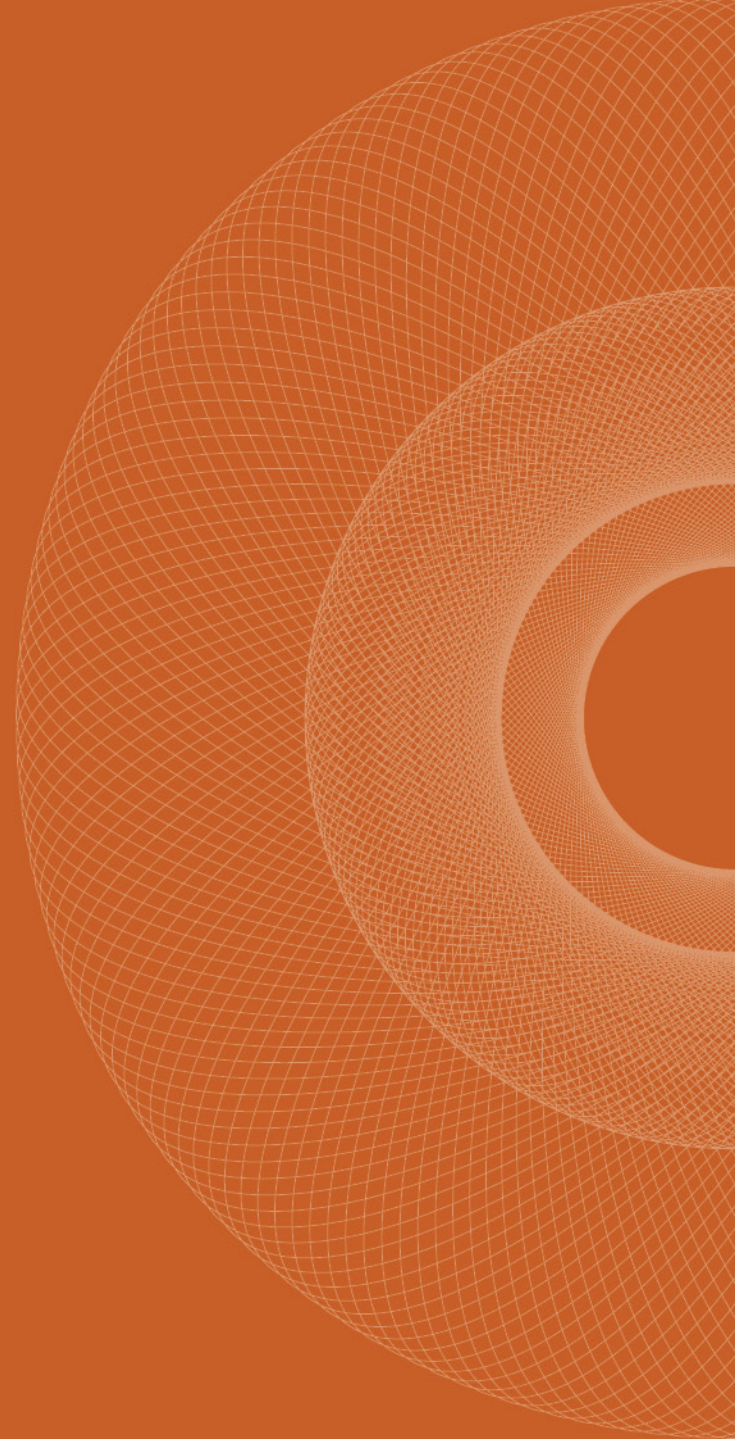


Špecificky navrhnutá ochrana osobných údajov – čl. 25 (1)

- Špecificky navrhnutá ochrana osobných údajov (*data protection by design*) znamená, že prevádzkovateľ musí pri (i) určovaní prostriedkov spracúvania ako aj (ii) počas samotného spracúvania implementovať bezpečnostné opatrenia, vzhľadom na
 - Najnovšie poznatky (*state of the art*) a náklady na implementáciu takých opatrení;
 - Povahu, rozsah, kontext a účely spracúvania osobných údajov;
 - Riziká zásahu do práv a slobôd fyzických osôb.
- Predovšetkým: pseudonymizácia a minimalizácia údajov



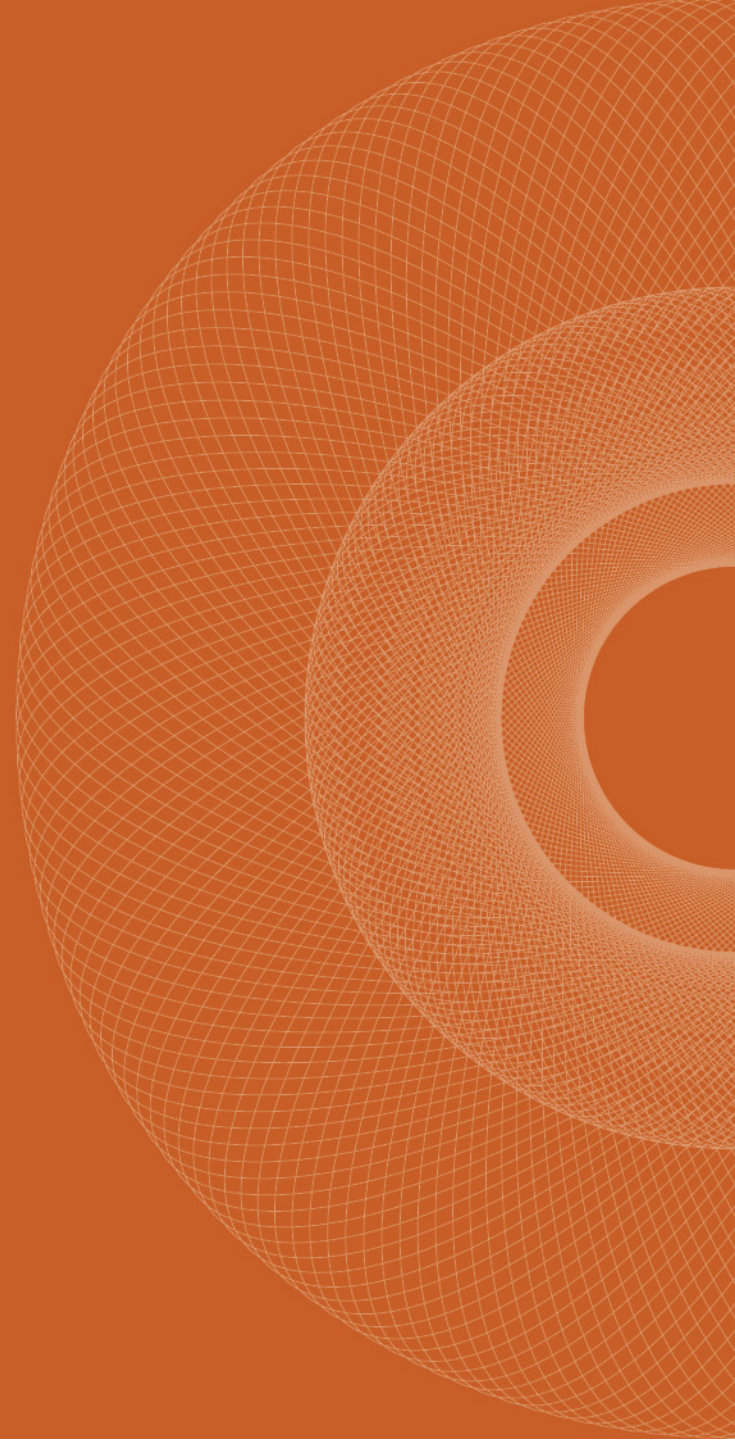
Porovnanie



Bezpečnostné opatrenia	Terajšia úprava	Nariadenie
Základná požiadavka	<i>Primerané</i> spôsobu spracúvania ako aj rizikám z toho vyplývajúcim	Berúc do úvahy <i>najnovšie poznatky (state of the art)</i> , náklady na ich <i>implementáciu</i> , okolnosti spracúvania a hroziace riziká (ktoré sa menia), <i>primerané bezpečnostné opatrenia</i>
Musia byť šité na mieru?	Áno, musia zodpovedať konkrétnym podmienkam spracúvania a rizikám	Áno, musia zodpovedať <i>najnovším poznatkom</i> , nákladom na <i>implementáciu</i> , okolnostiam spracúvania, účelu spracúvania, rizikám a to zároveň <i>v čase začatia ako aj počas spracúvania</i>
Bezpečnostný softvér	Bezpečnostný softvér dostupný na trhu sa musí brať do úvahy <i>len primerane</i>	Do úvahy sa musia zobrať <i>najnovšie poznatky (state of the art)</i> , berúc do úvahy náklady na jeho implementáciu, okolnosti spracúvania a hroziace riziká
Príklady bezpečnostného softvéru a povinnosť implementovať ho	Napr. šifrovanie, antivírus, antispam, firewall, ochrana proti hackerským útokom, pravidelné zálohovanie, legálny softvér, riadenie prístupu avšak povinnosť implementovať <i>len „primerane najmä“</i>	To isté + <i>pseudonymizácia</i> + povinnosť implementovať „ <i>ktoré zahŕňajú aj</i> “
Musia sa aktualizovať?	Áno, <i>ak nastali zmeny</i> pri spracúvaní osobných údajov	Áno, navyše <i>proces pravidelného testovania, hodnotenia a posudzovania účinnosti bezpečnostných opatrení</i>



Niektoré ďalšie zmeny



Pseudonymizácia

- Osobné údaje, ktoré sú pseudonymizované a umožňujú identifikáciu FO na základe ďalších informácií (kľúča) sú stále považované za osobné údaje;
- Ako sa posudzuje, či je možné FO identifikovať?
 - Berú sa do úvahy všetky prostriedky, pri ktorých existuje **primeraná pravdepodobnosť**, že ich daná osoba využije na identifikáciu FO;
 - Napr. možnosť vyselektovania, vzdialenosť kľúča od osoby, náklady a čas potrebný na identifikáciu, dostupná technológia a technologický rozvoj;
- **Kľúč by mal byť uchovávaný oddelene** od pseudonymizovaných údajov;
- Nariadenie upozorňuje, že online identifikátory vytvárané mobilnými zariadeniami, aplikáciami a protokolmi (napr. IP adresy, cookies) môžu zanechávať stopy, ktoré v kombinácii s ďalšími informáciami môžu viesť k vytváraniu užívateľských profilov a následnej identifikácii FO.
- Avšak, aj keď je možné FO identifikovať, samotné sťaženie identifikácie pseudonymizáciou je chápané ako nové bezpečnostné opatrenie.
- Otázka: je možné považovať pseudonymizáciu, šifrovanie (a antivírus) od výrobcov operačných systémov za primerané vzhľadom na najnovšie poznatky na trhu?

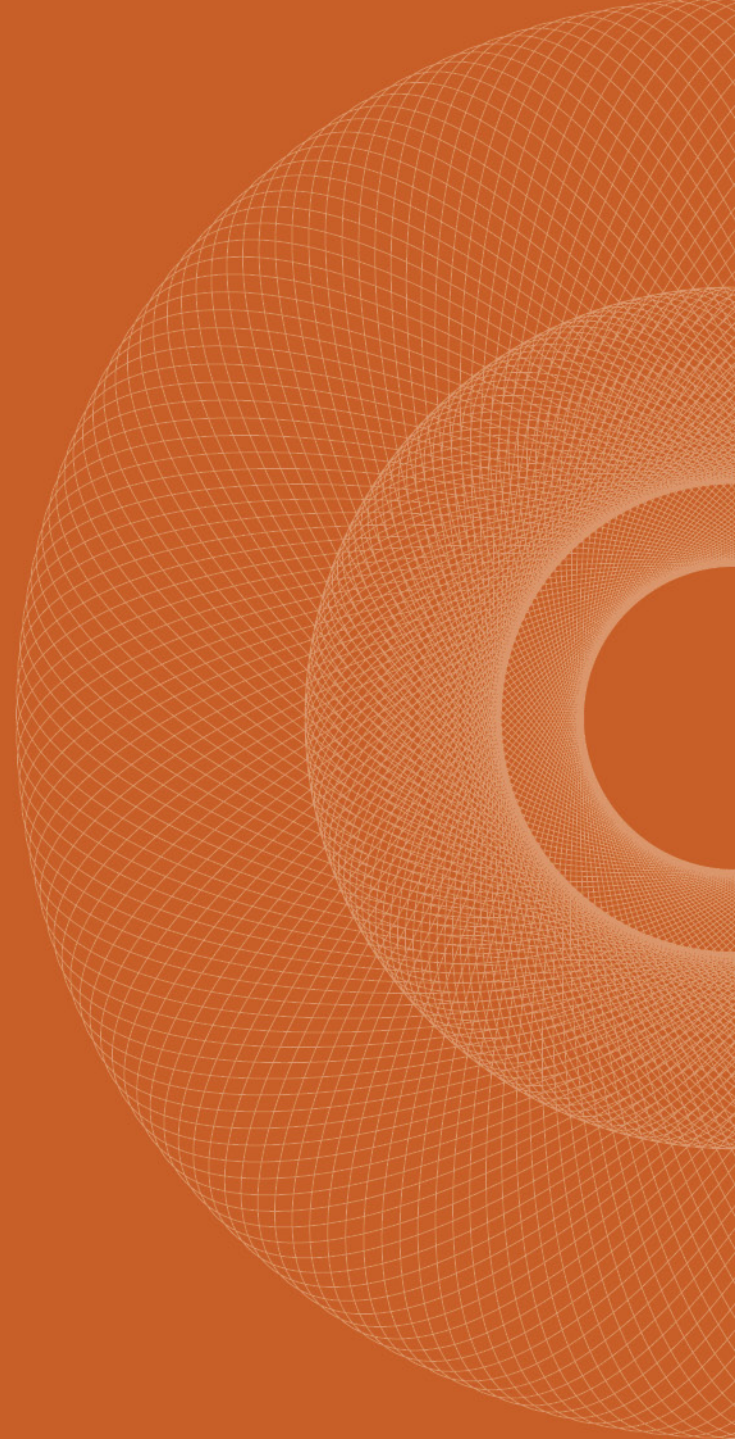
Posudzovanie vplyvu (*impact assessment*)

- V podstate ide o zvýšený štandard posudzovania rizík. V prípade, ak typ spracúvania údajov – najmä použitie nových technológií – pravdepodobne povedie k vysokému riziku pre práva FO.
- Prevádzkovateľ je v takom prípade povinný pred spracúvaním vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Ide najmä o prípady:
 - Systematického a rozsiahleho hodnotenia údajov založenom na automatizovanom spracúvaní údajov, vrátane profilovania, so závažným vplyvom na FO;
 - Spracúvania citlivých osobných údajov vo veľkom rozsahu;
 - Systematického monitorovania priestorov prístupných verejnosti vo veľkom rozsahu;
- Konzultácia s Úradom – ak by posúdenie vplyvu viedlo k záveru, že bez prijatia opatrení prevádzkovateľom by hrozilo vysoké riziko.
- Alebo ak by hrozilo vysoké riziko, ktoré prevádzkovateľ nemôže zmierniť primeranými opatreniami, pokiaľ ide o najnovšie technológie a náklady na vykonanie opatrení.

Nové práva dotknutých osôb

- Právo na prenosnosť údajov:
 - v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi;
 - iba ak je právny základ súhlas alebo plnenie zmluvy s dotknutou osobou;
 - právo na prenos osobných údajov od jedného prevádzkovateľa druhému, pokiaľ je to technicky možné.
- Právo na vymazanie (právo „na zabudnutie“):
 - ak boli zverejnené osobné údaje, prevádzkovateľ je povinný vymazať osobné údaje, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení;
 - a zároveň informuje iných prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.

Kde začat?



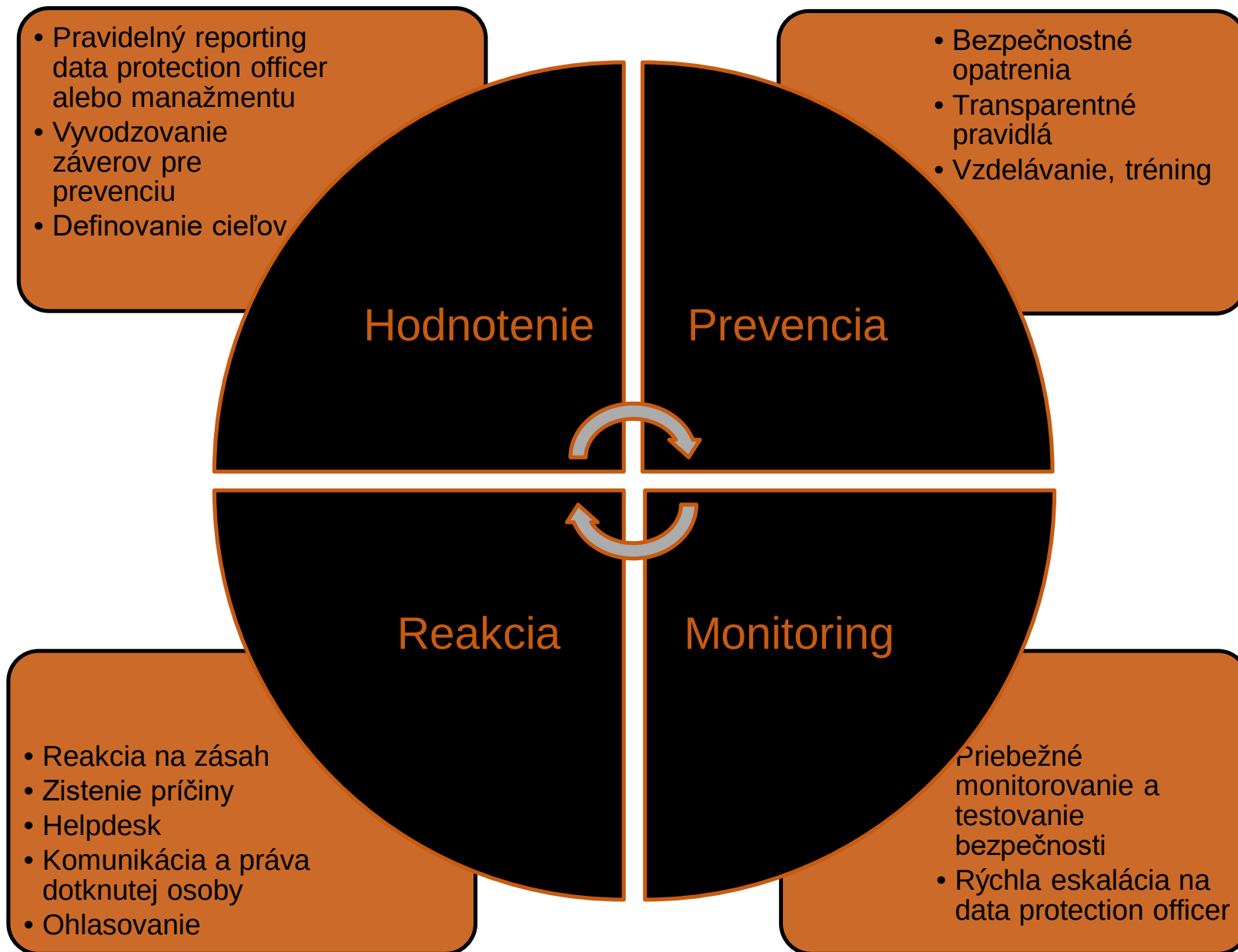
Kde začať?

Pár postrehov pred začatím:

- Súlad s Nariadením nie je jednorazová záležitosť, ale neustále prebiehajúci proces;
- Compliance 1.0 vs compliance 2.0;
- Požiadavka na pravidelné testovanie, posudzovanie a hodnotenie - cyklus;
- Reporting managementu – kontrola rizík spojených s vysokými pokutami;
- Predpripravte sa – požiadavka spolupráce do zmlúv.

Prvé kroky:

- Snaha o pochopenie a zmapovanie toku údajov v spoločnosti, t.j. definovanie základných účelov spracúvania, právnych základov spracúvania a postavenie jednotlivých osôb v tomto procese = data flow map
- Následne, snaha o reálne zabezpečenie ochrany údajov (najmä technickými prostriedkami);
- Snaha o budovanie robustného compliance programu – ako by mal vyzeráť?



Otázky?
Ďakujem za pozornosť.

Jakub Berthoty

Associate, Kinstellar

+421 2 5929 1126

jakub.berthoty@kinstellar.com