

GDPR a řízení rizik

Zbyněk Malý, DATACONS

*e*FOCUS

DATA 
CONS

GDPR

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 (všeobecné nariadenie o ochrane
údajov)

Osobní údaje mají vysokou hodnotu

Pojem osobní údaj

Pro účely tohoto nařízení se rozumí:

- „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“);
- identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

ÚČTY

MAJETEK

ZVYKY / ZÁJMY

RODINA / PŘÁTELÉ

IP ADRESY

JMÉNA

ADRESY

FOTKY

KARTY

EMAILY

Osobní
údaje mají
vysokou
hodnotu

CENA ?

DOPADY ?

RIZIKA ?

Finanční ztráty

Poškození značky

Narušení provozu

Pokuty

Incidenty s osobními daty



> 500 M accounts

únik: 2014
zveřejnění: 2016

Top 10 breaches		
 myspace	359,420,698	MySpace accounts
 in	164,611,595	LinkedIn accounts
 A	152,445,165	Adobe accounts
 hadoo	112,005,531	Badoo accounts  
 k	93,338,602	VK accounts
 b	68,648,009	Dropbox accounts
 umbln	65,469,298	tumblr accounts
 iMesh	49,467,477	iMesh accounts
 Fling.com	40,767,652	Fling accounts 
 last fm	37,217,682	Last.fm accounts

 Sensitive breach, not publicly searchable
 Unverified breach, may be fabricated

Incidenty s osobními daty

KIM ZETTER SECURITY D

T-Mobile má za únik dat 1,2 milionu klientů zaplatit pokutu 3,6 milionu



Úřad na ochranu osobních údajů pokutou „ocenil“ nedostatečné zabezpečení klientských dat. A konečně víme, co všechno T-Mobilu uniklo.



Česká spořitelna
autor: HN - Lukáš Bíba

Incidenty s osobními daty

Pokuta od ÚOOÚ (T-Mobile CZ 2016)

EURO

150 k

Pokuta GDPR (20 M EUR)

20 M

Pokuta GDPR (4% z obrátu TMCZ)

38,5 M

Pokuta GDPR (4% z obrátu DT)

2 920 M

Cíle GDPR

- Modernizovat – soulad s technologiemi
- Sjednotit pro celou EU (i mimo EU)
- Zvýšit ochranu, zlepšit kontrolu, zrychlit reakci

Proč je GDPR důležité

- GDPR se týká každého

zaměstnanci

zákazníci / klienti / občané / pacienti

- Celá řada změn, náročné splnění požadavků

- Pokuty – mohou být až likvidační

20 milionů EUR,

4 % celkového ročního obratu celosvětově

- Lhůta už běží, času je málo

Vstoupilo v platnost 25. května 2016

Toto nařízení se použije ode dne 25. května 2018.

Nejsložitější požadavky GDPR

- Právo výmazu
- Právo přenositelnosti
- Získávání souhlasu subjektů
- Předávání údajů do třetích zemí
- Ohlašování incidentů
- Provádění analýz rizik (DPIA)
- Pověřenec (DPO)

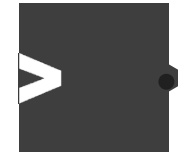
Otázky pro přípravu GDPR

- **Znáte všechna svá data?**



Datová inventura

- **Víte, kde všude jsou?**



Mapování dat a procesů

- **Víte, proč je zpracováváte?**



Hodnocení a řízení rizik

- **Víte, kdo a co s nimi dělá?**



IT Security nástroje

- **Znáte všechna rizika?**

- **Umíte je vyřešit?**



Incident management

GDPR – čím
začít?

Zahájení projektu GDPR



Analýza dat, stavu a nedostatků

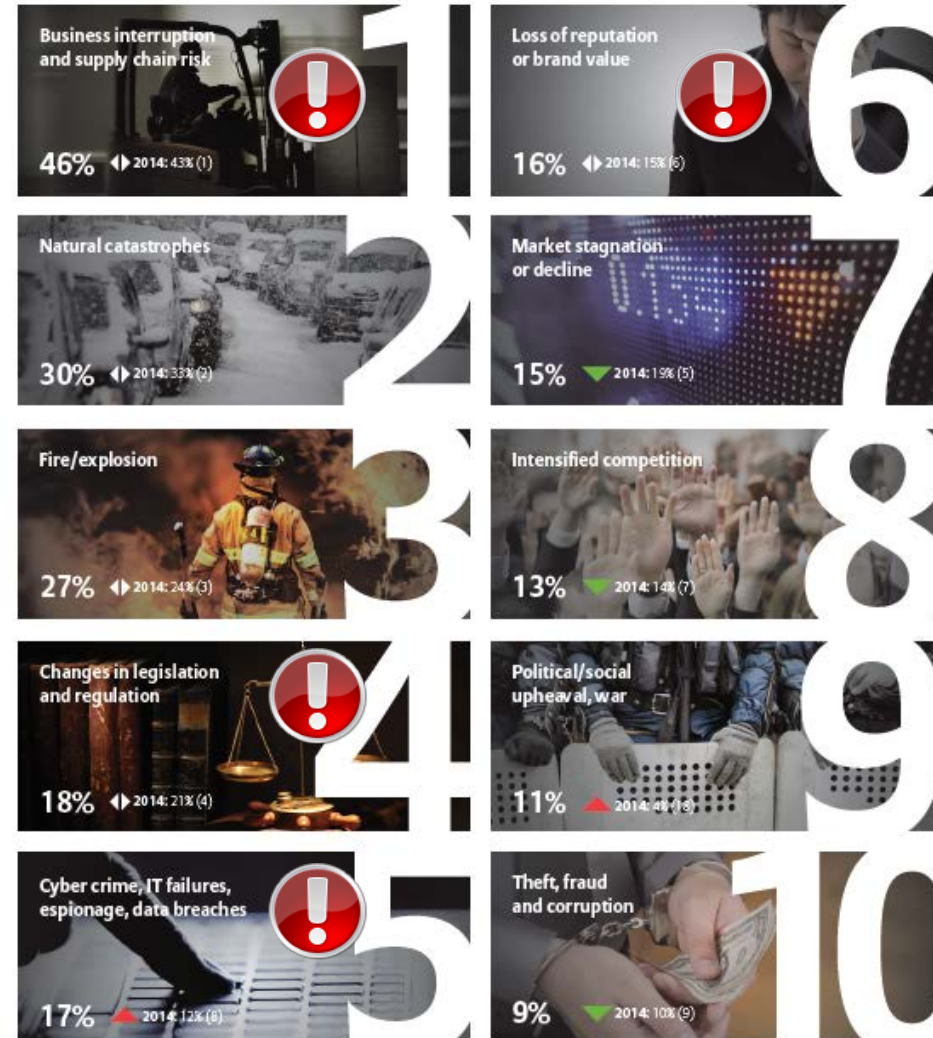


Implementace



Řízení rizik – důležitost kybernetických rizik

Top 10 Global Business Risks for 2015



To see full Risk Barometer 2015 rankings [click here](#)

Source: Allianz Global Corporate & Specialty. For methodology, see page 3

Řízení rizik & GDPR

- Odpovědnost správce
- Záměrná a standardní ochrana
- Zabezpečení zpracování
- Ohlašování případů porušení
- Oznamování případů porušení
- Posouzení vlivu na ochranu (DPIA)

Řízení rizik & GDPR

- Odpovědnost správce

- S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.

- Záměrná a standardní ochrana

- S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření.

Řízení rizik & GDPR

- Ohlašování případů porušení

- Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

- Oznamování případů porušení

- Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.

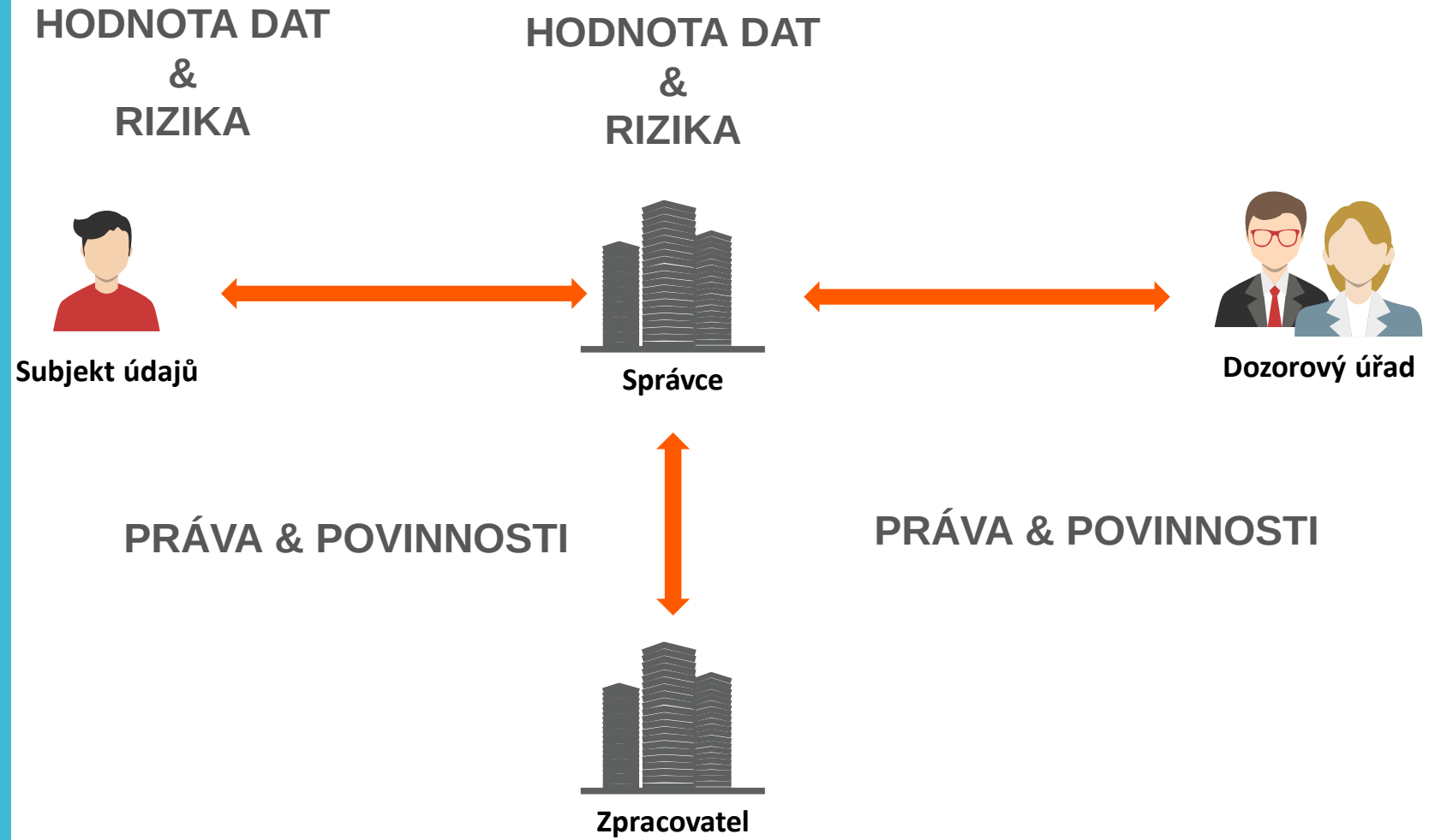
Řízení rizik & GDPR

- Posouzení vlivu na ochranu

(DPIA)

- Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

Vztahy v GDPR



Ďakujeme za pozornosť

