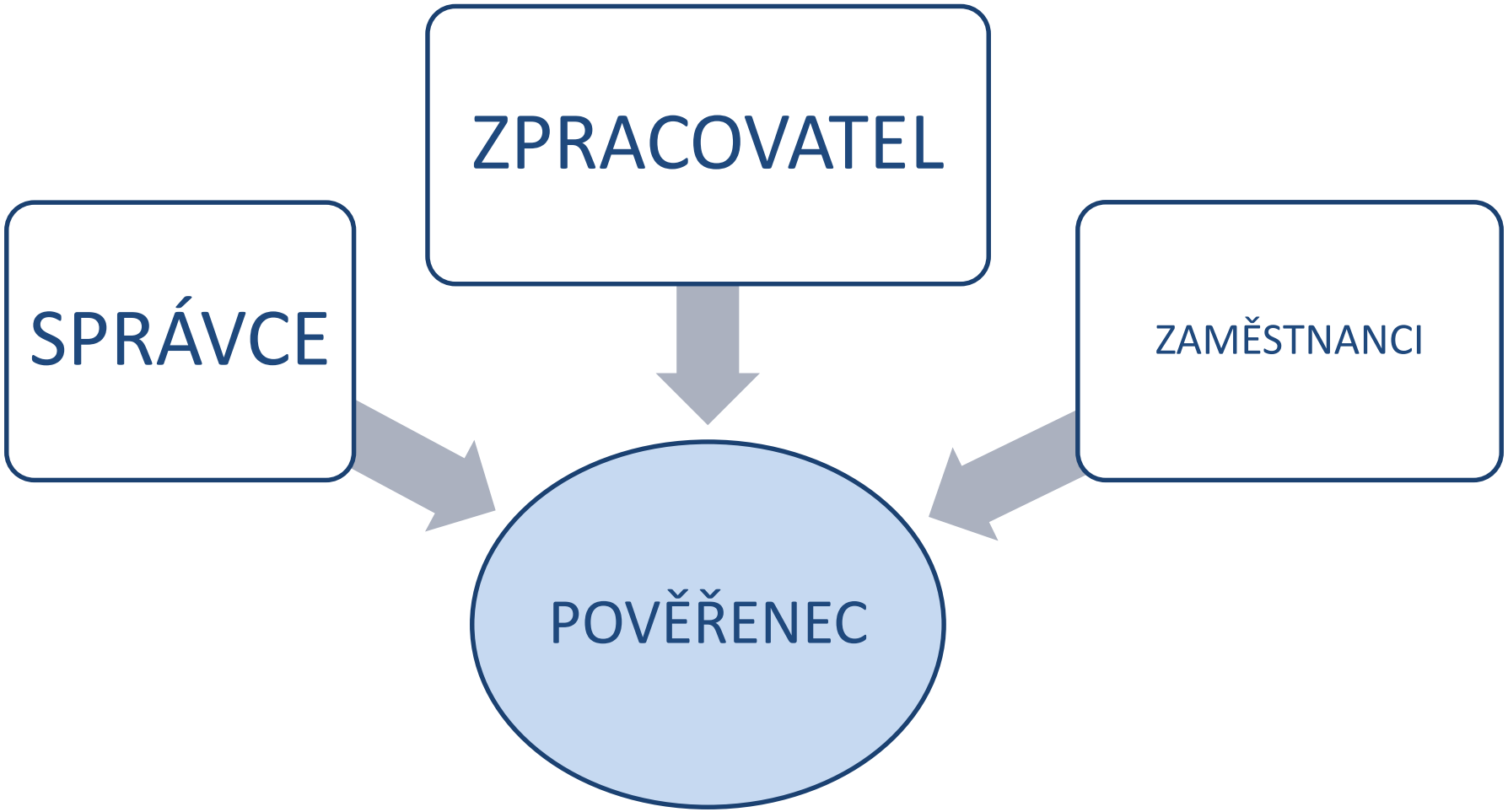
POVĚŘENEC OCHRANY OSOBNÍCH ÚDAJŮ, HROZBY A RIZIKA VE ŠKOLSTVÍ V PROBLEMATICE GDPR

Bc. Radek Kubíček, MBA

Praha 26. 03.2018

2K CONSULTING

ROLE POVĚŘENCE (DPO)



CO VŠE SOUVISÍ S POVĚŘENCEM ?

- Organizační zařazení pověřence a vztah pověřence a správce / zpracovatele
- V organizaci seznámení s procesy mapování, analýzy rizik, směrnicemi….
- Požadavky na odbornou znalost pověřence
- Konflikt zájmů pověřence
- Povinnosti pověřence

STŘET ZÁJMŮ PRO VÝKON POVĚŘENCE

Činnost pověřence nesmí provádět z interních zaměstnanců :

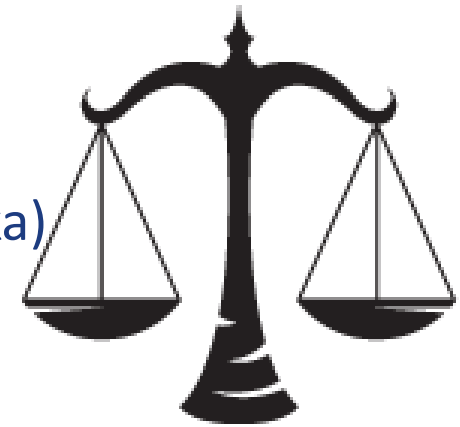
- Statutární zástupce organizace
- Personalista, účetní, IT technik, právník

U externího pověřence nesmí docházet ke smluvnímu vztahu s danou organizací při zpracování a nebo zajištění u FO a PO: viz. článek 38, odst.6.

a/ personalistiky, účetnictví a daňové poradenství

b/ právní služby a poradenství

c/ správa a údržba IT zařízení / dodavatel software (matrika)



= hrozí sankce za nedodržení pravidla o střetu zájmu.

ZÁKLADNÍ PRAVIDLA PRO ZAJIŠTĚNÍ ČINNOSTI POVĚŘENCE ČL.37

A. Pověřence musí mít každá instituce rozhodující o právech a povinnostech osoby
B. Pověřenec má být kvalifikovanou osobou, znalou právních předpisů na ochranu osobních údajů (včetně důkladné znalosti nařízení)
C. Pověřencem může být buď pracovník (tj. zaměstnanec školy), nebo externě spolupracující osoba.
D. Pověřenec má být nezávislý a nestranný, a proto nařízení mj. požaduje, aby:
    1. pověřenci nebyly udíleny žádné pokyny týkající se plnění jeho úkolů podle Nařízení
    2. pověřenec nebyl pro plnění svých úkolů propuštěn ani sankcionován (interní DPO)
    3. plnění jiných úkolů pověřence nevedlo ke střetu jeho zájmů
E. Pověřenec musí být přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele, resp. mít přímý přístup k vedení obce (školy) či příslušné organizace
F. Pověřenec pomáhá zajišťovat soulad činnosti zpracovatele nebo správce s právními předpisy na ochranu osobních údajů
G. Pověřenec musí být snadno dosažitelný pro obec (školu) , ÚOOÚ i veřejnost

POVĚŘENEC – ÚKOLY POVĚŘENCE OSOBNÍCH ÚDAJŮ ČL.39

Povinnosti :

a) Poskytování informací subjektům údajů

b) Poskytování poradenství na požádání pro DPIA

c) Působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, vedení konzultací k činnostem zpracování a jiných věcí.

d) Zapracovává a hodnotí riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování

e) Zvyšování povědomí a odborné přípravy pracovník zapojených do operací zpracování a souvisejících auditů.

f) Monitorování souladu s tímto nařízením a dalšími předpisy EU nebo členských států v oblasti ochrany údajů, pravidelné přenášení doplňujících informací pravidel pro nakládání s osobními údaji (legislativa)

g) Účastnit se celoživotního vzdělávání v oblasti informační a datové bezpečnosti (doklady o vzdělání součástí výroční zprávy o výkonu činnosti pověřence)

KVALIFIKAČNÍ PŘEDPOKLADY DPO (EXTERNÍ DPO, PRÁVNICKÁ OSOBA)

a) předložení seznamu členů realizačního týmu (IT specialista, auditor, pověřenec, právník).
b) garance zastupitelnosti (nemoc, dovolená atd.)
c) seznam referencí o výkonu činností dle zákona č. 101/2000 Sb., o ochraně osobních údajů a v souvislosti s novou legislativou – Nařízením Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR),
d) pracovní pohotovost 24/7 a garance dopravní dostupnosti v případě neodkladného řešení bezpečnostního incidentu (sídlo kanceláře, provozovny, pevná linka) – včetně víkendů a dnů pracovního klidu;
e) minimálně jeden kontrolní den v období dvou kalendářních měsíců, sepsání protokolu o provedení činnosti; zápis z porady vedení
f) certifikát nebo jiný doklad o vzdělávání pověřenců v oblasti GDPR

MÝTY A DOPORUČENÍ K VÝKONU POVĚŘENCE (EXTERNÍ DPO)

Nespoléhejte pouze na fyzickou osobu (OSVČ):

A. sdílený pověřenec – v případě kontroly na více místech současně, Vám nebude k dispozici.

B. Požadujte počet subjektů, kde již pověřence bude vykonávat. (existují i příklady, kdy jedna osoba má nasmlouvaných 80 subjektů)

C. Pověřence musí vykonávat i v místě subjektů údajů (nestačí poradenství po telefonu)

D. Komunikace prostřednictvím zabezpečených kanálů (datová schránka FO).

E. Požadujte reference a praxi v oblasti informační a datové bezpečnosti, auditorské činnosti v oblasti veřejné správy a školství.

= **pozor na střet zájmu, žádejte záruku ve smlouvě o zajištění výkonu pověřence apod.**

RIZIKA PŘI VÝKONU POVĚŘENCE

- Nedostatečná informovanost o rozhodnutích správce (pravidelné pracovní setkání)
- Porušení mlčenlivosti
- Nedostupnost
- Nedostatečná znalost organizace, jejich procesů a předpisů = nutnost seznámit se se vstupní auditem GDPR, analýzou rizik…
- Nedostatečná odborná znalost a praxe v oblasti informační a datové bezpečnosti, oblasti řízení rizik a auditní činnosti.

ANALÝZA RIZIK GDPR

- Je požadovaná při posouzení vlivu na ochranu osobních údajů podle článku 35 odstavce 7. Posouzení obsahuje alespoň :

a) Systematický popis zamyšlených operací zpracování a účely zpracování , případně včetně oprávněných zájmů správce.

b) Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů

c) Posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1

d) Plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

ANALÝZA RIZIK GDPR JE POŽADOVÁNA

– **Lze tedy provedením jedné analýzy rizik vyřešit povinnosti článku 24 i 35?**

= analýza rizik je důležitá z hlediska kontrol a doporučuje se jako součást metodiky analýzy rizik . Nutnost uvádět citace dle článku nařízení EU a norem 27 001 a 27005. Tato analýza musí být podle potřeby revidovaná a aktualizovaná.

ANALÝZA RIZIK GDPR – POVINNOSTI

- **Povinnosti uvést tento dokument :**

A) Vnitřní směrnice pro ochranu osobních údajů

B) Organizační řád školy - systém řízení rizik - informační a datová bezpečnost

C) Školení bezpečnosti informací – pro správce i zpracovatele

= důležitá je role pověřence pro ochranu osobních údajů, který vyhotovuje kontrolní záznamy o činnosti.

PROČ JE ANALÝZA RIZIK DŮLEŽITÁ?

- Při stanovení bezpečnostních a organizačních opatření pro jednotlivá zpracování osobních údajů podle článku 24, bodu 1 a 2.
- S přihlédnutím 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 zjistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením.

SPRÁVCE A ZPRACOVATEL – ANALÝZA RIZIK

SPRÁVCE

- FO nebo PO, která **určuje účel a způsoby zpracování**
- nese plnou **odpovědnost za zákonnost zpracování a soulad s GDPR**
- musí být **schopen soulad s GDPR doložit, vede evidenci bezpečnostních incidentů**
- nese **odpovědnost za škodu** ve vztahu **k subjektům dat**

ZPRACOVATEL

- FO nebo PO, který **zpracovává** data jménem správce a **výhradně na jeho pokyn**
- měl by správce upozornit na nezákonnost zpracování
- pracuje na základě **písemné smlouvy**
- **Nese odpovědnost za škodu při zpracování dat ve fyzické i elektronické podobě**

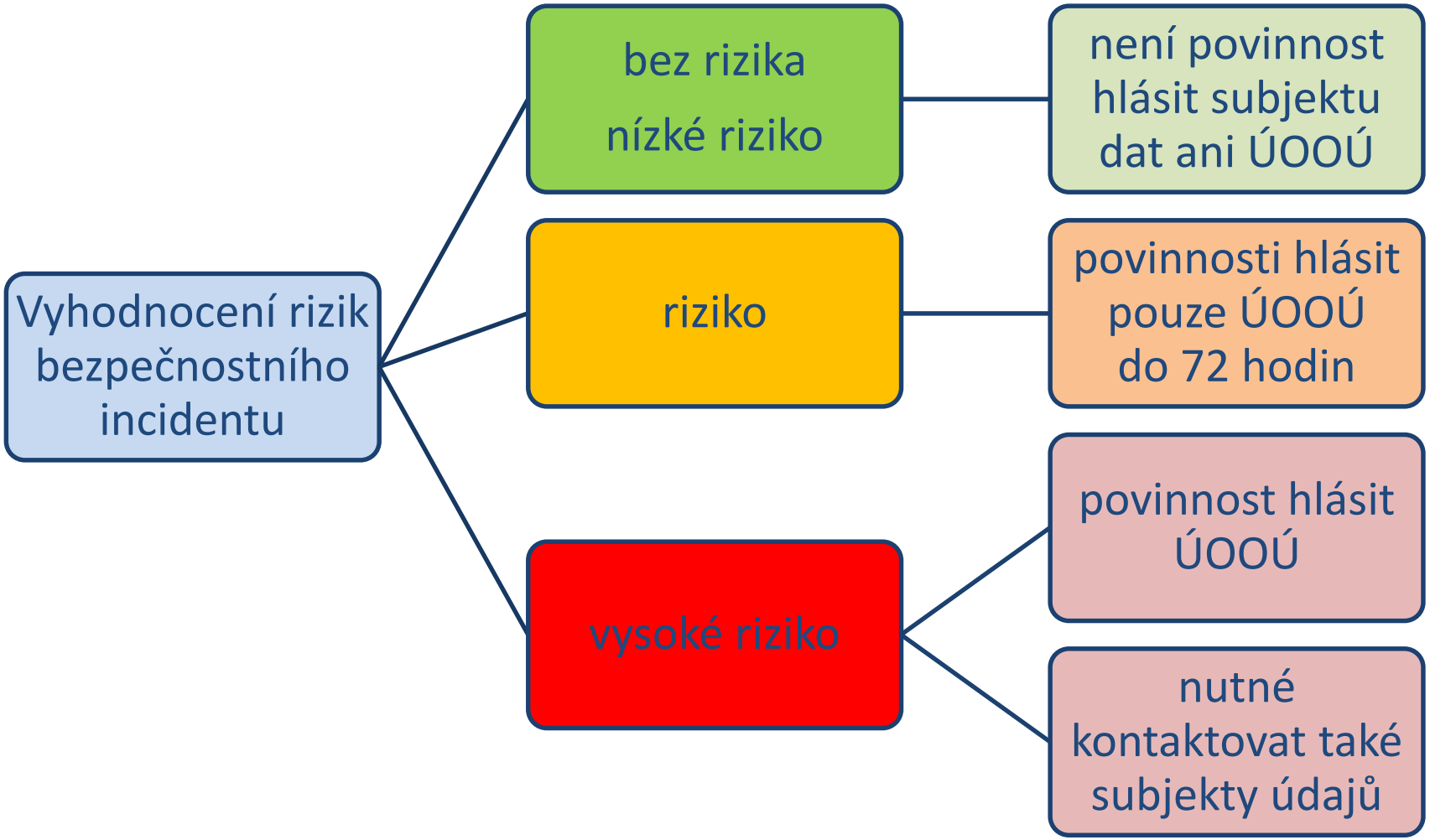
JAK ZPRACOVAT ANALÝZU RIZIK ?

- Metodika provedení analýzy rizik :

a) ISO 27 001 a 27 005 / Systémy řízení bezpečnosti informací
b) Přílohy č.2 vyhlášky č.316 /2014 Sb. vyhláška o kybernetické bezpečnosti.
c) § 4, odst 4 až 7 vyhlášky viz výše.

Analýza rizik nedá se udělat dle šablony, každá organizace má jiná aktiva a na základě této analýzy bude muset přijmout odlišná organizační, procesní a technická opatření. Součástí metodiky musí být i katalog hrozeb pro různé oblasti bezpečnosti.

OHLAŠOVACÍ POVINNOST



SEZNAM BEZPEČNOSTNÍCH INCIDENTŮ – HROZEB / KYBERNETICKÁ BEZPEČNOST

- Hardware (nedostatečné postupy likvidace)
- Software (nedostatečné testování programů, neodhlášení při opuštění pracovní stanice, chybné přiřazení přístupových práv, nechráněné tabulky s heslem, nedostatečné zálohování)

SEZNAM BEZPEČNOSTNÍCH INCIDENTŮ – HROZEB / FYZICKÁ BEZPEČNOST

- Nedostatečná fyzická ochrana budov, dveří, oken

- Nepřiměřená nedbalá kontrola fyzického přístupu do budov, místnosti, kanceláří (spisovna, serverovna atd.)

SEZNAM BEZPEČNOSTNÍCH INCIDENTŮ – HROZEB / ZAMĚSTNANCI

- Nedostatečné bezpečnostní školení v oblasti GDPR
- Nedostatek povědomí o bezpečnosti
- Nedostatek kontrolních mechanismů
- Nedostatečná kontrola práce externích zaměstnanců nebo zaměstnanců zabezpečujících úklid

SEZNAM BEZPEČNOSTNÍCH INCIDENTŮ – HROZEB / ORGANIZACE

- Nedostatečný formální postup při registraci a zrušení registrace uživatele (bývalý zaměstnanec).
- Nedostatečný formální postup při revizi uživatelských práv (přístup do školní matriky mají všichni stejná práva)
- Nedostatečné nebo neúplné zajištění bezpečnosti ve smlouvách se dodavateli nebo třetích stran (zpracovatelská smlouva)
- Nedostatečné provádění pravidelných auditů / interní zaměstnanec (pověřenec)
- Nedostatečné nebo neúplné zajištění bezpečnosti ve smlouvách se zaměstnanci (odpovědnost za škodu a trestněprávní odpovědnost fyzických osob)
- Nedostatečně definované povinnosti informační bezpečnosti v popisu pracovních pozic (revize pracovních smluv, školení bezpečnosti informací).

CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI

- podcenění nestrukturovaných dat a dat v listinné podobě

CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI

- odemčené počítače v nepřítomnosti na pracovišti

- ponechání dokumentů s os. údaji bez dozoru

CLEAR DESK POLICY

CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI

- Neznalost/ neuvědomění si rizik v organizaci
- Nezpracování analýzy rizik na klíč dané organizaci
- Neproškolení v oblasti bezpečnostní informací = výstupem je kontrolní test.

CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI

- práce na nezabezpečených lokálních úložištích
- neprověřené datové nosiče, otevřené porty
- využívání nezabezpečených komunikačních kanálů

CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI

- nesprávná archivace a likvidace dokumentů

DĚKUJI ZA POZORNOST

Bc. Radek Kubíček, MBA

2K CONSULTING s.r.o.

Specialista řízení rizik ve školství

775 110 979

radek.kubicek@2kconsulting.cz

2K CONSULTING