MUNI
LAW

DPIA v praxi

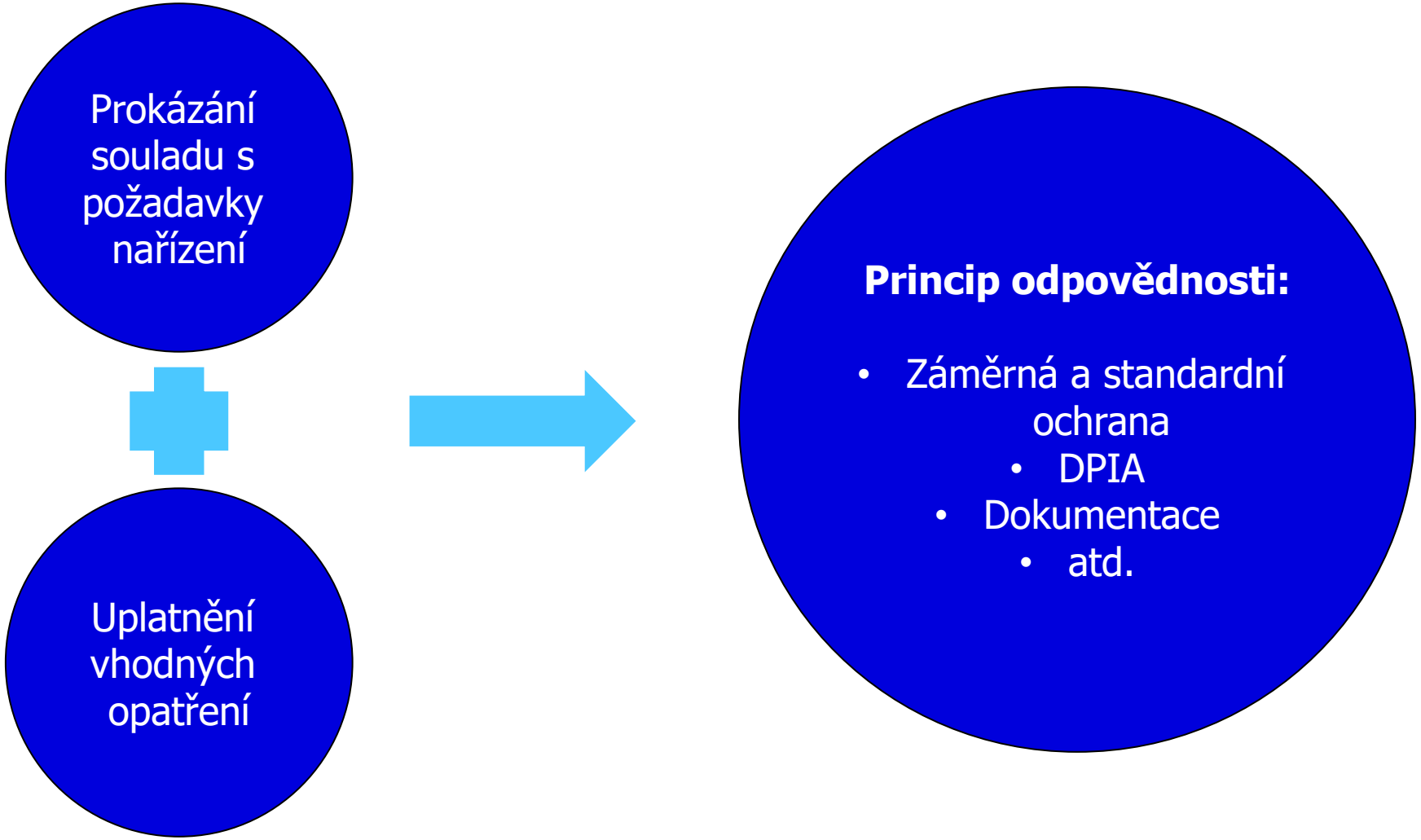
Václav Stupka

Agenda

- Co je DPIA
- Co říká právní úprava
- Jak na to

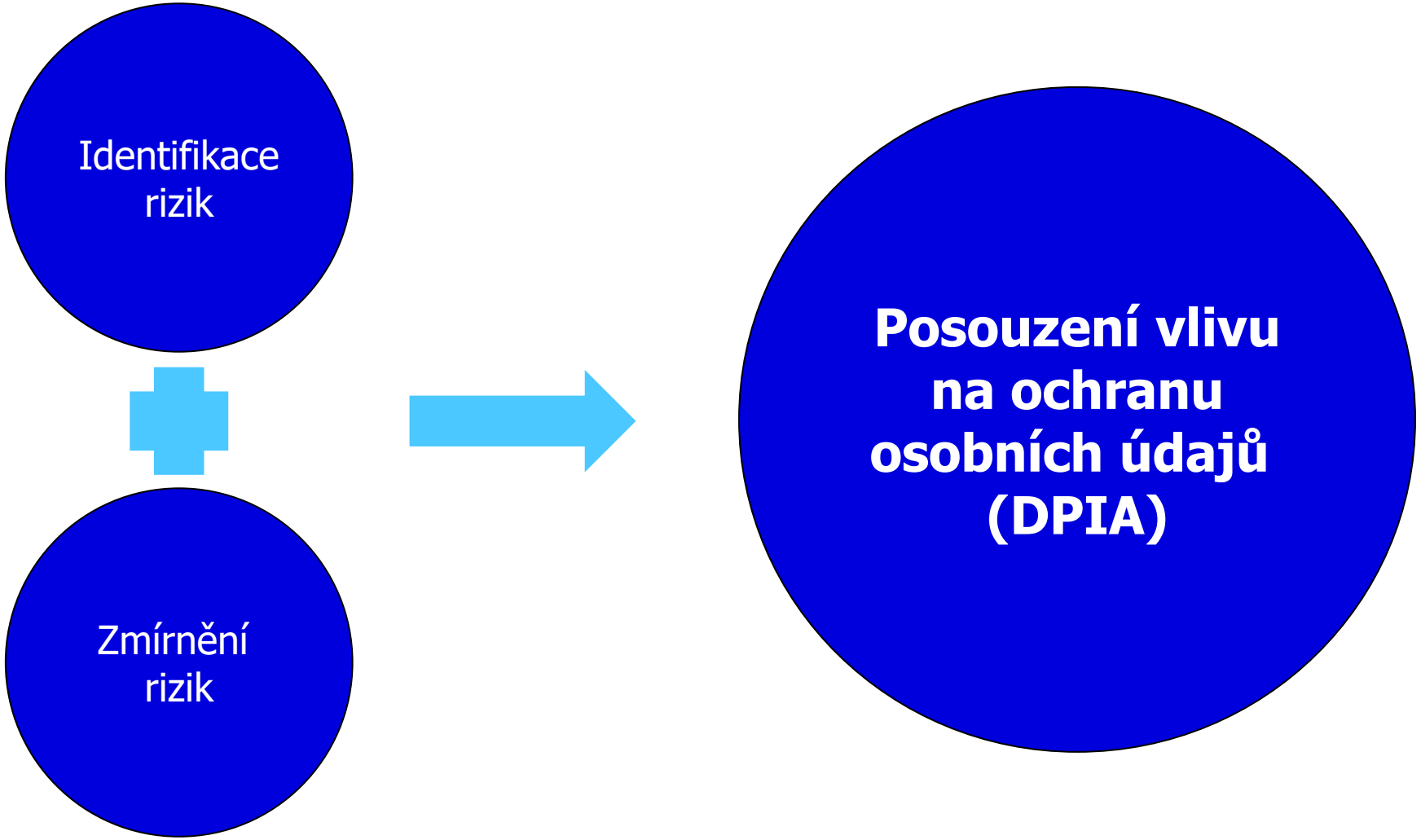
MUNI LAW

Princip odpovědnosti



MUNI LAW

Princip odpovědnosti



MUNI LAW

Co je DPIA

- Posouzení vlivu (zpracování) na ochranu osobních údajů
- Dokumentovaný proces v rámci kterého je hodnocen vliv zpracování na práva a svobody subjektů údajů
- Lze se inspirovat ISO/IEC 29134 – DPIA je ale obecnější
- Hodnotí se riziko třetí osoby

MUNI
LAW

Co říká právní úprava

Kdy je nutné DPIA

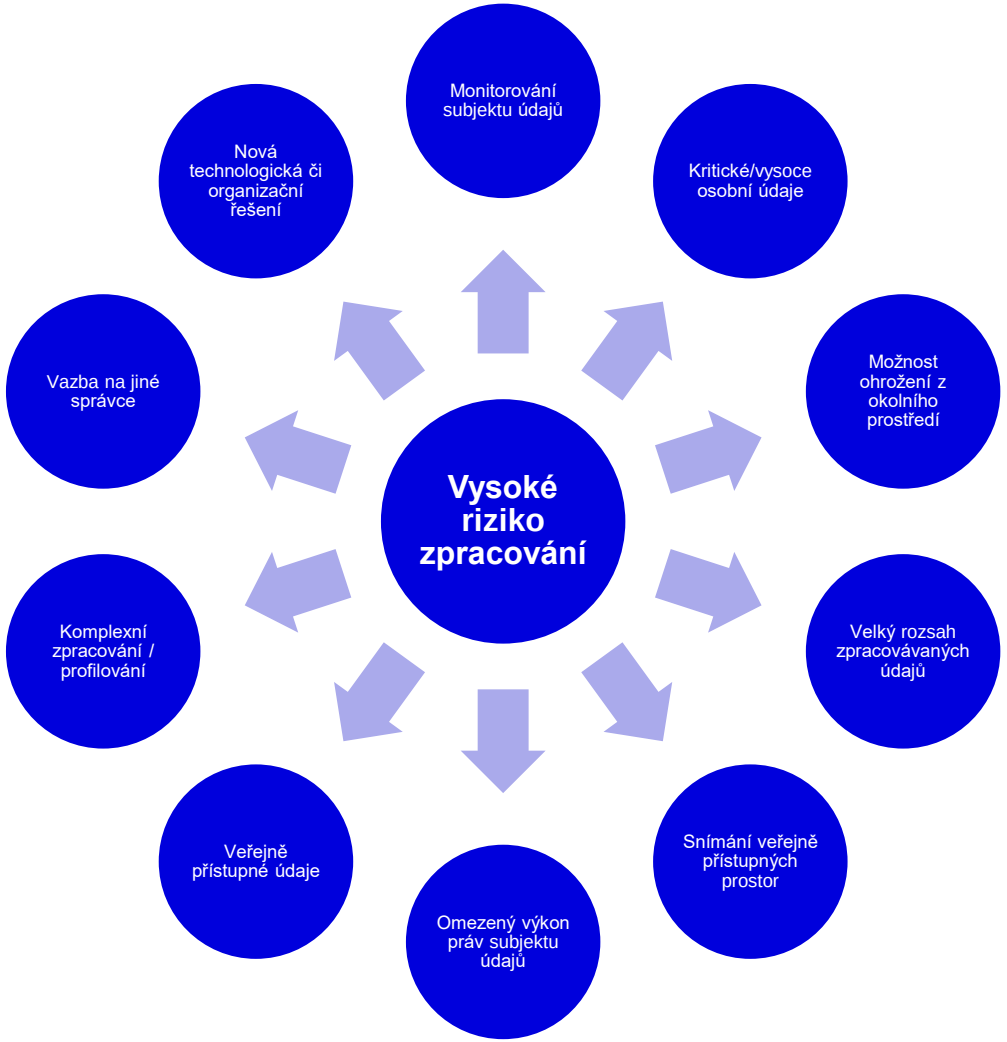
- „Vysoké riziko pro práva a svobody subjektu údajů“
- ÚOOÚ: seznam druhů zpracování vyžadujících DPIA
- Výjimky:
  - Seznam druhů zpracování nevyžadujících DPIA
  - Zákonné zpracování a DPIA už zpracované bylo
  - Typově podobné zpracování, kde DPIA už proběhlo
  - Úřad už provedl kontrolu

MUNI LAW

Vysoké riziko

MUNI LAW

Vysoké riziko



MUNI LAW

Obsah DPIA

- Popis operací zpracování a jeho účely
- Posouzení účelnosti a přiměřenosti operací zpracování
- Posouzení rizik pro práva a svobody subjektu údajů
- Opatření k řešení identifikovaných rizik

MUNI LAW

MUNI
LAW

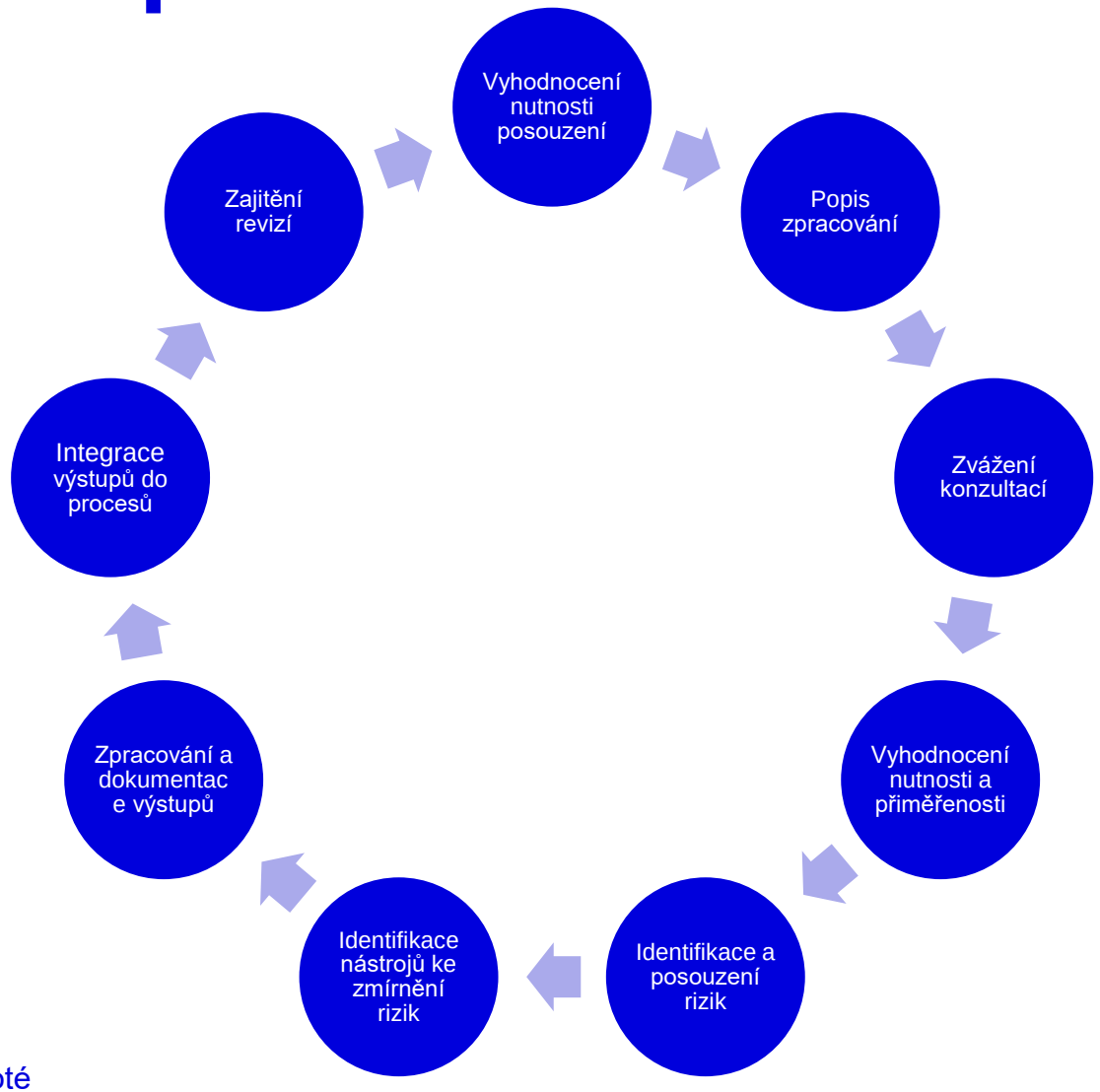
Jak na to?

Zohlednění cílů

- Ochrana práv a svobod subjektu
- Minimalizace dat
- Dostupnost
- Integrita
- Důvěrnost
- Nespojování
- Transparentnost
- Ovlivnitelnost

MUNI LAW

Vhodný postup



MUNI LAW

Vyhodnocení nutnosti posouzení

- Vedle vodítek k posouzení zpracování s vysokým rizikem je vhodné zohlednit:
  - Povahu zpracování
  - Rozsah zpracování
  - Kontext zpracování
  - Účely zpracování
- Někdy může být DPIA užitečné i když není povinné

MUNI LAW

Určení zpracovatele a sběr podkladů

- DPIA obecně provádí správce – lze určit kteroukoliv odpovědnou osobu (kromě pověřence)
- Vhodné podklady (právní úprava, interní normy a instrukce, metodiky, organizační struktura, dodavatelé, dokumentace ICT systémů a infrastruktur, atd.)

MUNI LAW

Popis zpracování

- Je vhodné dokumentovat údaje z předchozího kroku:
  - Povahu zpracování
  - Rozsah zpracování
  - Kontext zpracování
  - Účely zpracování
- Komplexní mapování informačních toků
- Funkční dekompozice
- Komponentová dekompozice

MUNI LAW

Konzultace

- Pověřenec – povinně
- ÚOOÚ – volitelně
- V rámci organizace
- Mimo organizaci

MUNI LAW

Vyhodnocení nutnosti a přiměřenosti

- Jak dopomáhá zpracování dosažení účelu?
- Existuje jiný postup jak dosáhnout stejného cíle?
- Je vhodné rovněž vyhodnotit další otázky compliance (právní základ, kvalita a minimizace dat, informace subjektům, výkon práva subjektů, povaha zpracovatelů, apod.)

Identifikace rizik

- Hledáme rizika v kontextu práva a svobod subjektu!
- Příklady rizik:
  - Nemožnost výkonu práv
  - Nemožnost přístupu ke službám
  - Diskriminace
  - Krádež identity
  - Ztráta kontroly nad osobními údaji
  - Finanční ztráty
  - Poškození reputace
  - Fyzická újma
  - Ztráta důvěrnosti, atd.

Vyhodnocení rizik

- Klasický přístup k hodnocení rizik:
  - Pravděpodobnost výskytu
  - Významnost dopadu
- Matice pro hodnocení rizik
- Vhodné je rovněž vyhodnotit rizika pro organizaci

MUNI LAW

Jak na rizika

- Modifikace rizika
- Vyloučení rizika
- Sdílení rizika
- Přijetí rizika

MUNI LAW

Volba nástroje ke zmírnění rizika

- Nutné zohlednit:
  - Povahu rizika
  - Zdroj rizika
  - Co je ohroženo
- Organizační, technická, právní opatření…
- Zohlednění cíle
- Přijetí reziduálního rizika

MUNI LAW

Dokumentace

- Popis jednotlivých kroků a jejich výstupů
- Stačí relativně stručná zpráva
- Plán integrace opatření (vč. odpovědnosti a termínů)
- Plán revizí (ne závazný – vazba na podstatné změny)

MUNI LAW

Závěr

- Není potřeba to přehánět
- Nemusí jít o strašáka, ale o pomocníka
- Neexistuje závazná podoba

MUNI LAW

MUNI
LAW

Díky za pozornost!

stupka@ics.muni.cz