

# **Bludiště na cestě k přiměřenému zabezpečení zpracování osobních údajů**

František Kasl

Ústav práva a technologií

Právnická fakulta

Masarykova Univerzita

09/2017

# Obsah

Labyrint práv a povinností

Nevyhnutelný vstup do bludiště

Zrcadlový labyrint?

Orientační body namísto mapy

Pohyblivé zdi

Mnoho cest

Představa pohledu z ptačí perspektivy

Ariadnina niť

Myší dírka

Závěr

# Labyrint práv a povinností

- **GDPR**

- blíže k regulované samoregulaci, celoevropské harmonizaci a usnadnění postupů dozorčího orgánu
- **zajištění přiměřeného zabezpečení zpracování os. údajů (čl. 24, čl. 32)**
  - dlouhodobě inherentní součástí úpravy ochrany osobních údajů
- povinnost doložit soulad s nařízením - **záznamy o koncepci realizovaných opatření**
  - porozumění smyslu a účelu úpravy
  - => schopnost kriticky posoudit přiměřenost
  - **důraz na kontinuální kontrolu**



# Nevyhnutelný vstup do bludiště

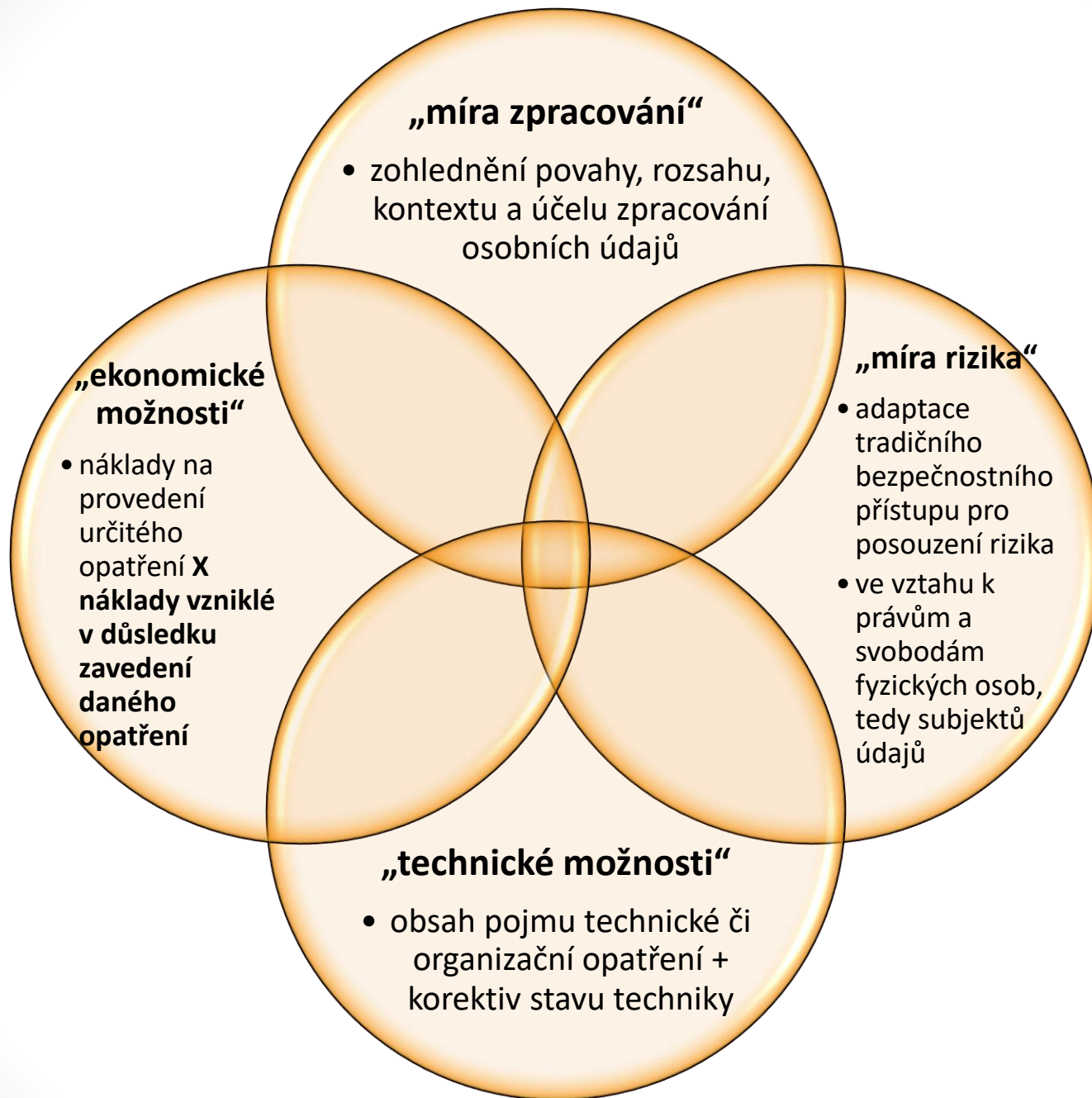
- zajištění vhodných a přiměřených technických a organizačních opatření pro zabezpečení zpracování osobních údajů
  - povinnost, jejíž náplň se odvíjí od identifikovaného rizika
  - již dnes **každý správce a zpracovatel osobních údajů**
  - >> **narušení bezpečnosti osobních údajů + kybernetických rizik**
  - **rostoucí provázanost IT a zprac. os. údajů**
  - v důsledku riziko **i pro důvěryhodnost a fungování entity**
- nevyhnutelné administrativní zatížení
- X nasměrování k zavedení **opatření s přidanou hodnotou pro široké spektrum subjektů**



# Zrcadlový labyrint?

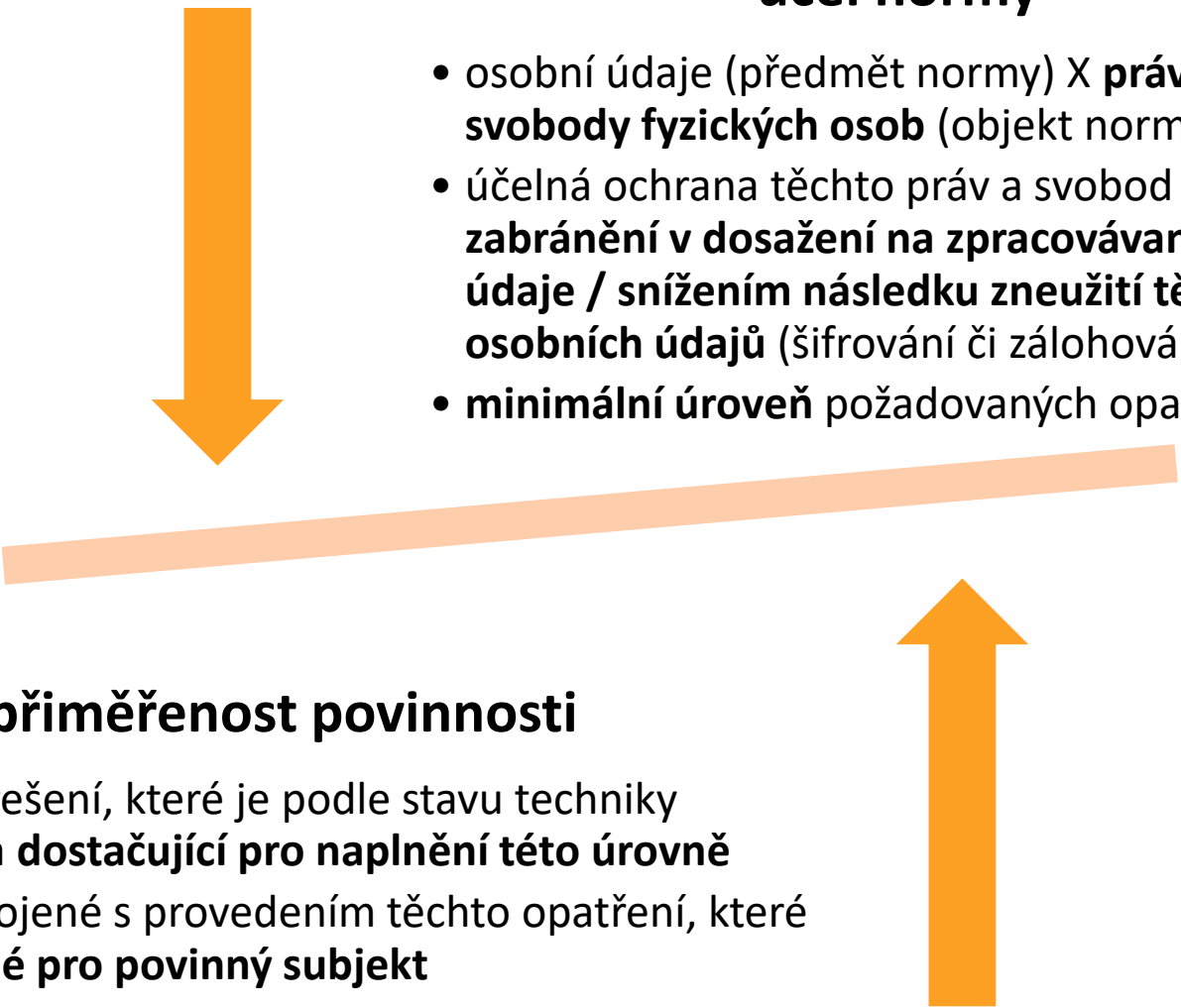
- GDPR vs Směrnice - projasnění situace
  - **významná kritéria**
  - **relevantní rizika**
  - **příkladná opatření**
  - **balanční mechanismy pro systematický přístup**
- **multipolárně strukturovaná norma**
  - zhodnocení situace na více osách současně
- paralela k systematické posouzení vlivu na ochranu osobních údajů dle článku 35 GDPR





# Orientační body namísto mapy

## účel normy

- 
- osobní údaje (předmět normy) X **práva a svobody fyzických osob** (objekt normy)
  - účelná ochrana těchto práv a svobod - **zabránění v dosažení na zpracovávané osobní údaje / snížením následku zneužití těchto osobních údajů** (šifrování či zálohování)
  - **minimální úroveň** požadovaných opatření

## přiměřenost povinnosti

- technické řešení, které je podle stavu techniky dostupné a **dostačující pro naplnění této úrovně**
- náklady spojené s provedením těchto opatření, které jsou **únosné pro povinný subjekt**

# Pohyblivé zdi

- prostředí informačních technologií je **v neustálém pohybu**
  - změny ve funkcích a možnostech nových technologií
  - proměna a vývoj kybernetických hrozeb
  - změny ve zpracování os.údajů
- **zajištění dynamické úrovně ochrany**
- potřeba **kontinuity a adaptability procesu**
  - srovnatelné s požadavky kybernetické bezpečnosti informačních sítí a zařízení
- náležité vybudování korporátní architektury  
+ kontinuální monitorování a aktualizace  
=> **usnadnění dodržování dalších povinností**





# Mnoho cest

**volnost při volbě konkrétní strategie a výběru dílčích opatření**

**spektrum dostupných nástrojů široké**

opatření pro kontrolu přístupu  
k zařízením;

opatření pro kontrolu nosičů  
údajů;

opatření pro kontrolu  
uložených osobních údajů;

opatření pro kontrolu  
přenosu;

opatření pro zajištění obnovy  
či hlášení chyb;

opatření pro ochranu  
osobních údajů před chybami  
ve fungování systému

**technologická neutralita**

konkrétní pro  
kombinace z  
pohledu dozorčího  
orgánu  
nerozhodná

rozhodné je  
dosažení  
přiměřené úrovně  
ochrany

**samoregulace**

kodex chování  
osvědčení



# Představa pohledu z ptačí perspektivy



## **potřebný systematický přístup**

- zdůrazněn komplexitou a provázaností s dalšími povinnostmi
- požadavky a postupy v rámci kybernetické bezpečnosti / specifické úpravy daného sektoru či povahy subjektu



## **potřeba širšího pohledu pro formulaci vhodné strategie**

- zpracování osobních údajů v souvislosti s dalšími požadavky a povinnostmi
- přizpůsobení postupů a mechanismů tomto specifickému mixu regulatorních požadavků pro daný subjekt



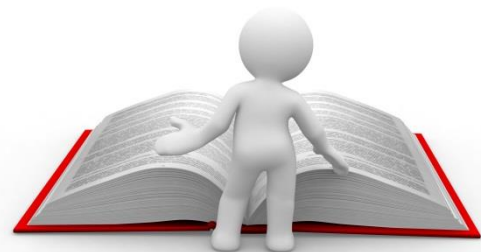
# Ariadnina niť

- **možnost sankčního postihu** ze strany dozorčího orgánu
  - **X doložení přiměřenosti opatření na základě dostupné dokumentace**
    - obecný popis přijatých opatření (apř. formou diagramu koncepce či organizační mapky)
- nadcházející regulatorní praxe Úřadu pro ochranu osobních údajů otevřenou otázkou
  - nejasné požadavky na menší správce a zpracovatele
  - lze však očekávat, že absence dokladů o přijatých opatřeních bude postihována sankčním opatřením



# Myší dírka

- dokumentační povinnost dle čl. 30 by se **neměla nevztahovat na malé a střední podniky**
  - X skutečný okruh subjektů významně zúžený = v prostředí digitální ekonomiky v podstatě pominutelná výjimka
    - podnik musí nejen fungovat s méně jak 250 zaměstnanci, **ale zároveň**
    - nesmí zpracovávat údaje intenzivněji než příležitostně,
    - ani přitom nesmí vznikat riziko pro práva a svobody subjektů údajů,
    - ani zpracovávat údaje spadající do zvláštních kategorií
  - zřejmě nebyl záměr normotvůrce = **následným výkladem pravděpodobně dojde k rozšíření výjimky**
- **povinnost dokumentace x zavedení opatření**



# Závěr

- **výkladová pomůcka**
  - **zdůraznění komplexity procesu**
    - multipolárně strukturovaná norma
    - „míra zpracování“; „míra rizika“; „technické možnosti“; „ekonomické možnosti“
  - **upozornění na souvislosti či spojitosti**
    - účel normy - přiměřenost povinnosti
    - zajištění dynamické úrovně ochrany
    - technologická neutralita
    - situace malých a středních podniků
    - systematický přístup a provázanost s dalšími povinnostmi
    - provázanost s kyberbezpečností a vlastním zájmem povinné entity
- reálná podoba těchto procesů u jednotlivých správců či zpracovatelů se může zásadně lišit
- rozbor systematiky ustanovení = pochopení jeho účelu a smyslu => **cesta k překlenutí výkladových nejednoznačností či neurčitostí**

Děkuji za  
pozornost!

