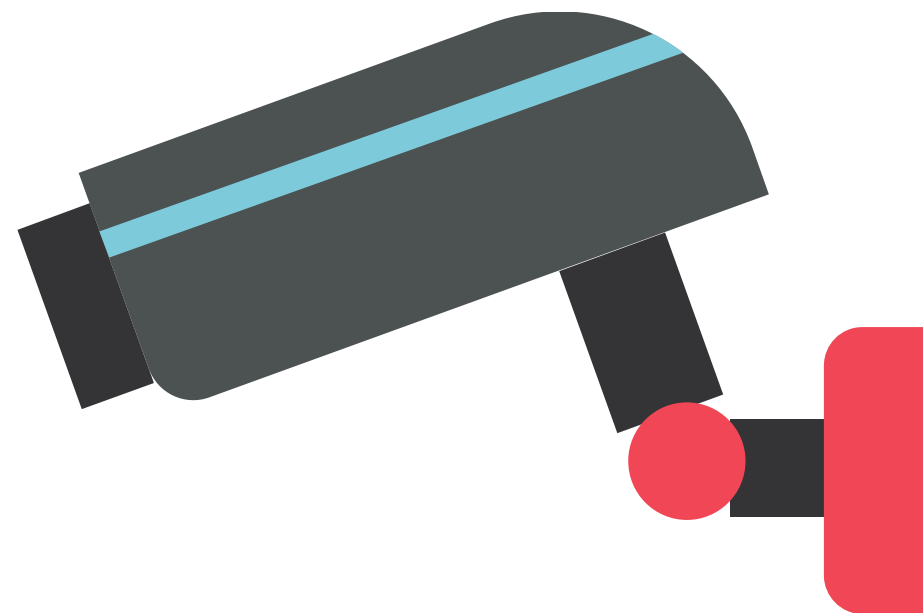


Osobní údaje v lékárnách

ΞΞ holubova.cz



GDPR

A world map with a dark blue background. Several countries are highlighted in a lighter blue color, including the United States, Canada, the United Kingdom, France, Germany, Italy, Spain, Portugal, Greece, Turkey, India, China, Japan, South Korea, Australia, and New Zealand. White curved lines connect these highlighted countries, suggesting data flow or global connectivity.

General Data Protection Regulation

Obsedné nařizení o ochraně osobních údajů

Evropská směrnice

- Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Zákon č. 101/2000 Sb., o ochraně osobních údajů

Evropské nařízení

- GDPR
- doprovodné zákony

**GDPR má přednost
před zákony.**

25. května 2018



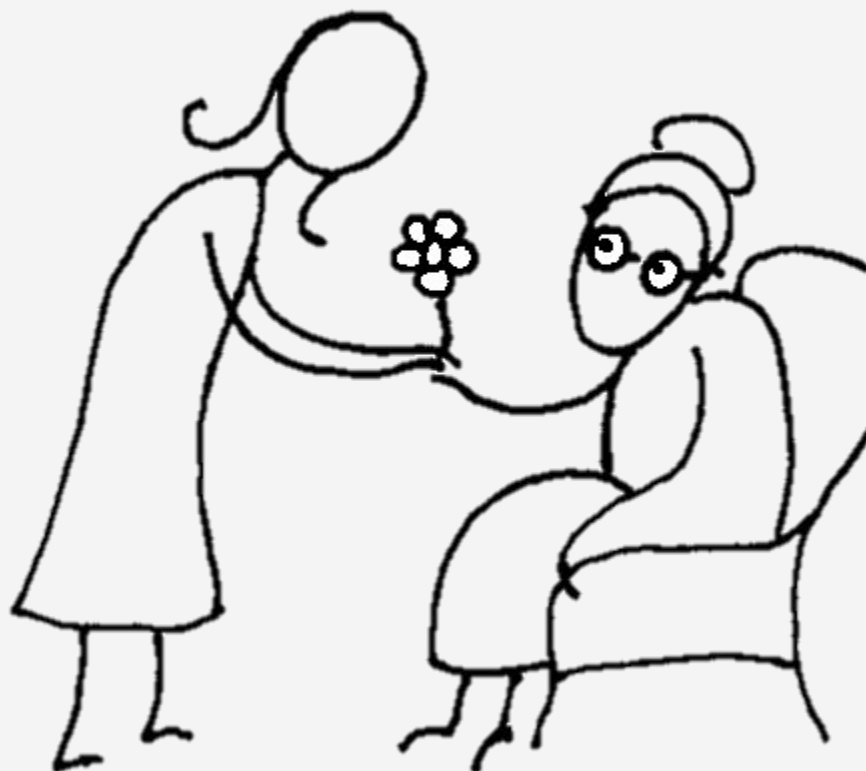


4,25 mio CZK





3,6 mio CZK





Karta klienta v sesterně

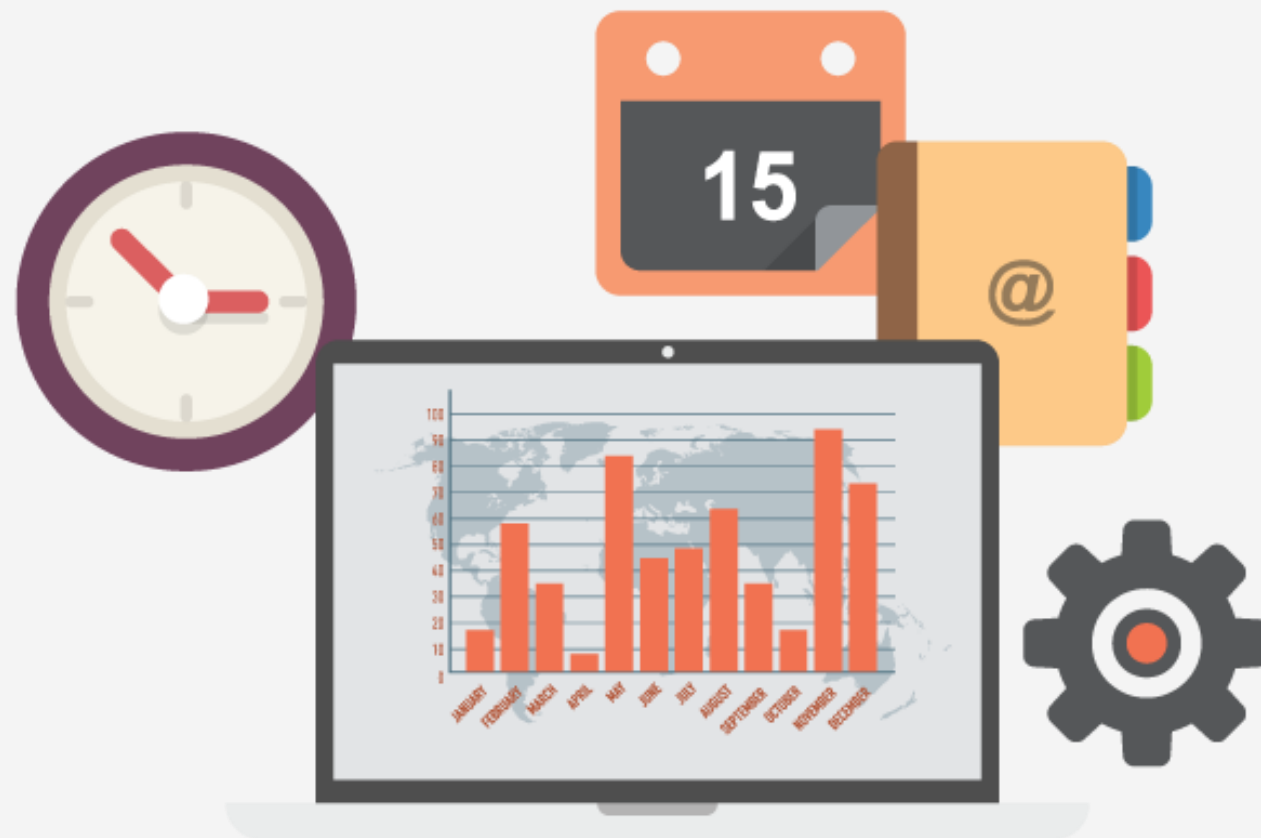
Pokuty dle GDPR

1. Odrazující
2. Účinné
3. Přiměřené



Na jaké zpracovávání se GDPR vztahuje?

1. Automatické
2. Manuální



Týká se GDPR Vás?



- 1. Zpracováváte osobní údaje klientů?
- 2. Monitorujete veřejně přístupné prostory kamerami?
- 3. Sledujete auta zaměstnanců přes GPS?
- 4. Zpracováváte osobní data zaměstnanců?
- 5. Sbírá Váš software místa pohybu, osobní údaje, IP adresy?

Kontrola aktuálních
vnitřních procesů

Texty souhlasů se
zpracováním a odvolávání

Právo na přístup
k osobním údajům

Pověřenec pro ochranu
osobních údajů (DPO)

Děti

Právní základ pro
zpracování

Posouzení vlivu na ochranu
osobních údajů (DPIA)

Ostatní firmy ve
skupině a v EU

Volba příslušného úřadu v EU

Úniky dat
a procesy



Tak postupně...

Obsah přednášky

1. Základní pojmy GDPR
2. Právní důvody zpracování osobních údajů
3. Práva a povinnosti v GDPR
4. Zabezpečení osobních údajů
5. Nové povinnosti
6. Pověřenec pro ochranu osobních údajů a jiné specifické povinnosti správce
7. Shrnutí

1. Základní pojmy

Osobní údaj

- jakákoliv informace o určené nebo určitelné fyzické osobě



Zvláštní kategorie osobních údajů

1. Rasový či etnický původ
2. Politický názor
- 3. Náboženské vyznání**
4. Filozofické přesvědčení
5. Členství v odborech
6. Genetické údaje zpracované za účelem jedinečné identifikace FO
7. Biometrické údaje zpracované za účelem jedinečné identifikace FO
- 8. Zdravotní stav**
9. Sexuální život nebo sexuální orientace

Zpracování osobních údajů

Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, např.

- shromáždění
- zaznamenání
- uspořádání
- strukturování
- uložení
- přizpůsobení nebo pozměnění
- vyhledání,
- nahlédnutí
- ...

Ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování, **pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. (15 GDPR)**

Osoby v GDPR

1. Subjekt údajů
2. Správce
3. Zpracovatel

Zásady zpracování

1. Transparentnost
2. Vymezený účel
3. Minimalizace
4. Doba uložení
5. Zabezpečení

Úkol 1

Lékárna jako zaměstnavatel požaduje poté, co uzavřela pracovní smlouvu se zaměstnancem, kopii rodného listu jeho dětí, a to za účelem plnění účetních povinností (konkrétně uplatnění slevy na dani). Posudte dle zásad v GDPR.

2. Právní důvody zpracování

Právní důvody zpracování běžných OÚ

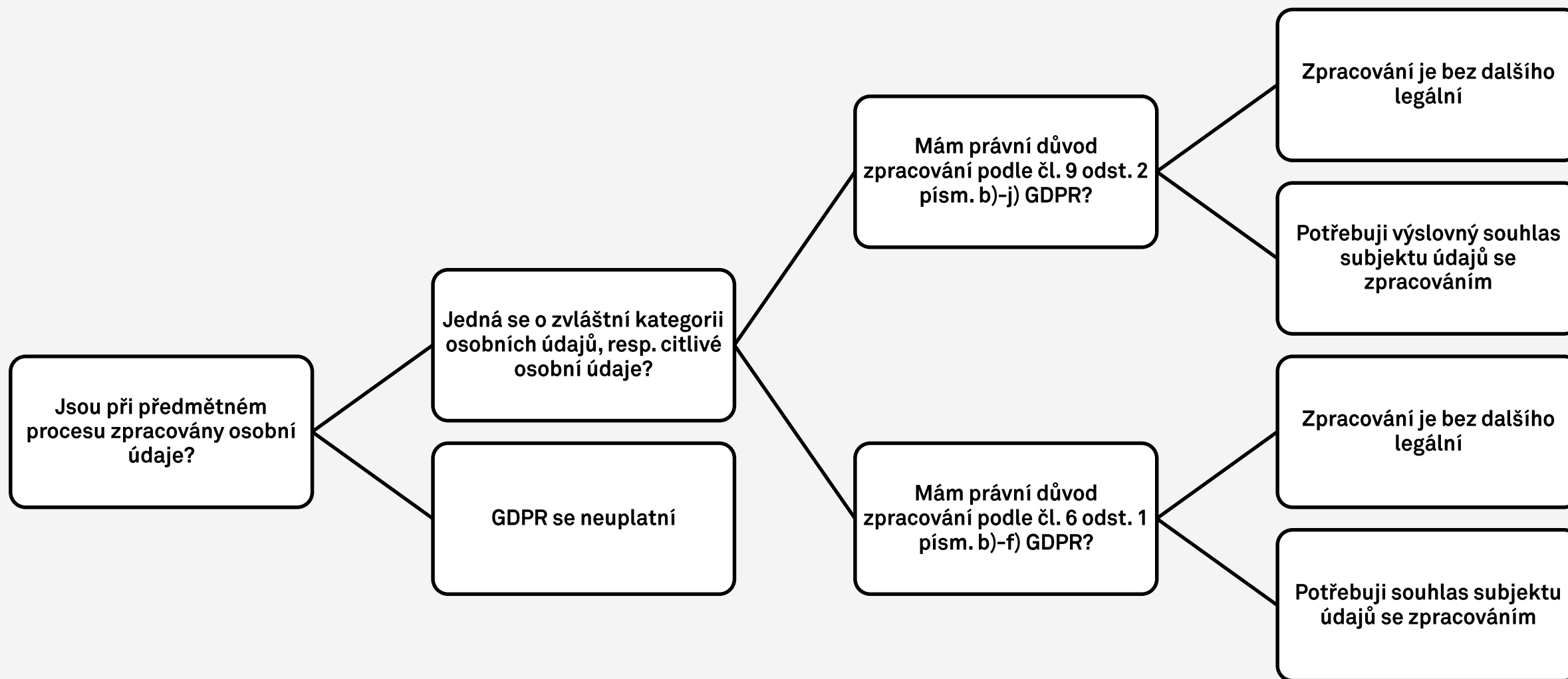
1. Smlouva
2. Zákon
3. Životně důležitý zájem
4. Veřejný zájem
5. Oprávněný zájem správce
6. Souhlas

I. Právní důvody zpracování citlivých OÚ

1. Výslovný souhlas
- 2. Nezbytné pro účely pracovního práva a sociálního zabezpečení**
- 3. Ochrana životně důležitých zájmů**
4. Zpracování prováděné nadací apod.
- 5. Údaje zjevně zveřejněné subjektem údajů**

II. Právní důvody zpracování citlivých OÚ

- 6. Nezbytné pro soudní řízení
- 7. Významný veřejný zájem
- 8. Preventivní, pracovní lékařství apod.**
- 9. Veřejné zdraví
- 10. Archivace ve veřejném zájmu apod.



Náležitosti souhlasu

1. Svobodný
2. Konkrétní
3. Informovaný
4. Nepodmíněný

Souhlas

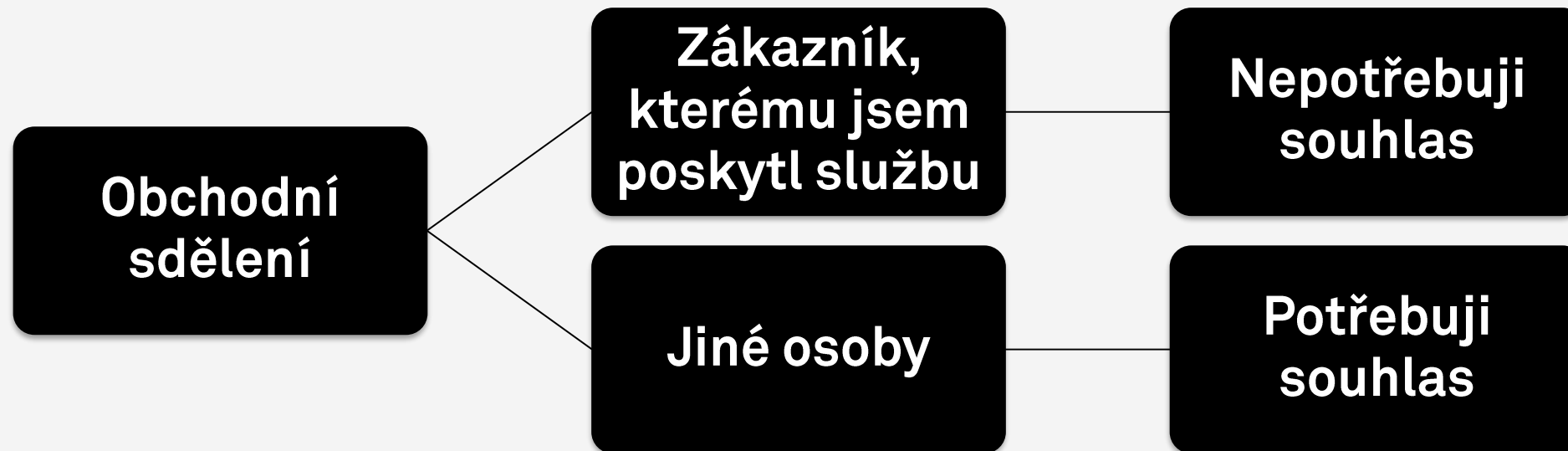
Informovaný

- podle zákona o zdravotních službách
- podle občanského zákoníku
- podle Úmluvy o biomedicíně
- podle školského zákona
- aj.

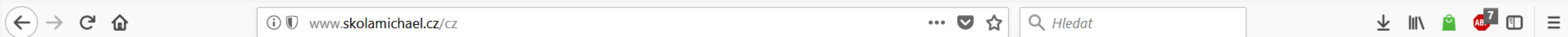
se zpracováním osobních údajů

- podle GDPR

Zasílání obchodních sdělení



Cookies



K personalizaci obsahu a reklam, poskytování funkcí sociálních médií a analýze naší návštěvnosti využíváme soubory cookie. Informace o tom, jak náš web používáte, sdílíme se svými partnery působícími v oblasti sociálních médií, inzerce a analýz.

Rozumím

ŠKOLA
MICHAEL

Střední škola a Vyšší odborná škola
reklamní a umělecké tvorby

SŠ

VOŠ

Aktuality

O škole

Fotogalerie

Projekty a stáže

Práce studentů

Kontakt



Česky ▼

Úkol 2

Váš klient Vám zaslal e-mail, ve kterém děkuje za doporučený lék, že mu velmi pomohl. Vy obsah e-mailu spolu se jménem klienta zveřejníte na svých webových stránkách v záložce reference. Posudíte, jak byste měli postupovat.

3. Práva a povinnosti v GDPR

Práva „na vyžádání“

Čl. 15 – 23 GDPR

Práva subjektu údajů

1. Právo na přístup k údajům
2. Právo na opravu
3. Právo být zapomenut
4. Právo na omezení zpracování
5. Právo na přenositelnost
6. Právo nebýt subjektem automatizovaného rozhodování dle profilování

Právo být zapomenut

1. osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
2. subjekt údajů odvolá souhlas
3. osobní údaje byly zpracovány protiprávně
4. osobní údaje musí být vymazány ke splnění právní povinnosti
5. osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti

Práva „bez vyžádání“ tzn. automatická Čl. 12– 14 GDPR

Čl. 13: OÚ získané od subjektu údajů

1. totožnost a kontaktní údaje správce;
2. kontaktní údaje pověřence pro ochranu osobních údajů;
3. účely zpracování a právní základ;
4. (oprávněné zájmy správce);
5. příjemci OÚ;
6. úmysl předat OÚ do třetí země

Čl. 14: OÚ nezískané od subjektu údajů

1. totožnost a kontaktní údaje správce;
2. kontaktní údaje pověřence pro ochranu osobních údajů;
3. účely zpracování a právní základ;
4. (oprávněné zájmy správce);
5. příjemci OÚ;
6. úmysl předat OÚ do třetí země

Jak na to?

1. Zásady ochrany OÚ na webových stránkách;
2. VOP;
3. Přihlášky a jiné dokumenty

Ukládání a nakládání s osobními údaji

1. Zabezpečení
2. Úložiště v EU a mimo EU
3. Předávání

Předávání osobních údajů

1. V rámci EU



1. Transparentnost

2. Mimo EU



1. Transparentnost
2. Zabezpečení
3. Poučení o (ne)existenci
rozhodnutí EK

Úkol 3

Držitel Vaší klientské karty Vám zaslal e-mail, že přechází k jiné lékárně a že tímto realizuje právo být zapomenut. Co byste měli udělat?

4. Zabezpečení

Hlediska vhodného zabezpečení

1. stav techniky
2. náklady na provedení
3. povaha, rozsah, kontext a účel zpracování
4. pravděpodobnost a závažnost rizika

Zabezpečení musí odpovídat riziku!

Doporučené způsoby zabezpečení dat

1. Anonymizace
2. Pseudonymizace
3. Šifrování

Takto ne!





holubova.cz







Ve zkratce

1. Fyzická ochrana datového centra, papírových dokumentů, monitoring tisku
2. Pravidelné update systémů, antiviry, firewalls, honeypots, ...
3. Zálohy dat ze serverů, PC, mobilních zařízení
4. Zajištění dostupnost pomocí duplikace systémů, monitoringu
5. Autentizace a autorizace uživatelů IS
6. Šifrovaná komunikace mezi systémy, vzájemná autentizace systémů
7. Data uložena na bezpečných místech (šifrování)
8. Pozor na USB disky, mobilní zařízení, emailovou komunikaci

Úkol 4

5. Nové povinnosti

I. Záznamy o činnostech zpracování

Všichni vyjma

- Méně než 250 zaměstnanců
 - + zpracování je příležitostné
 - + zpracování nepředstavuje riziko pro práva a svobody
 - + zpracování nezahrnuje zvláštní kategorii osobních údajů

**Lékárny musí vést záznamy o činnostech
zpracování**

II. Záznamy o činnostech zpracování

- Jméno + kontaktní údaje správce
- Účely zpracování
- Popis kategorií subjektu údajů a oú
- Kategorie příjemců
- Předání do třetí země
- Lhůta pro výmaz
- Technické a organizační bezpečnostní opatření

[illegible]

Posouzení vlivu na ochranu osobních údajů

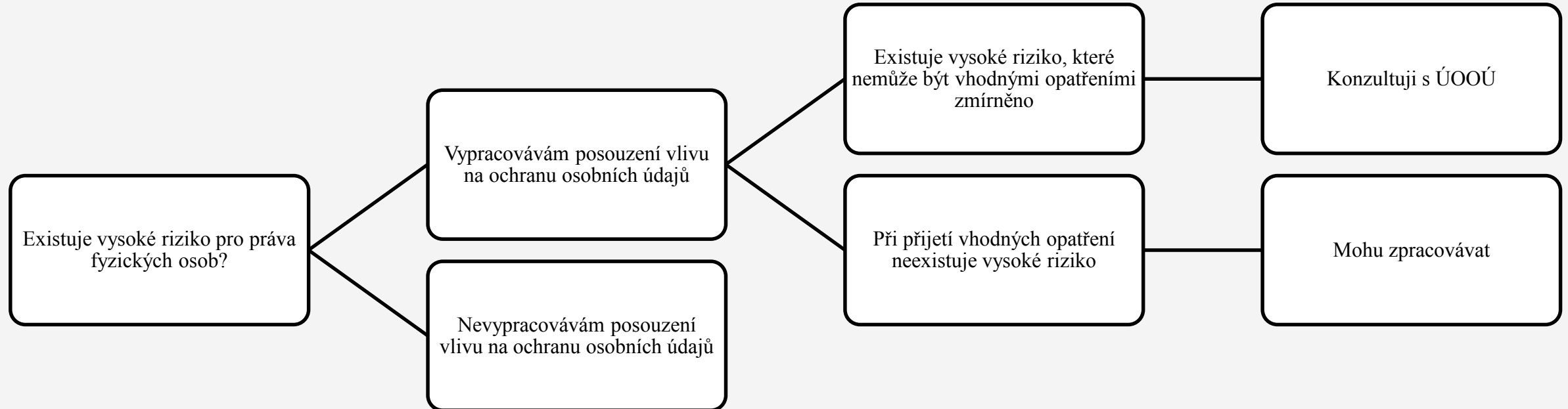
Vysoké riziko pro práva a svobody fyzických osob

- Monitorování veřejně přístupných prostor
- Rozsáhlé zpracování zvláštních kategorií údajů
- Systematické vyhodnocování osobních aspektů

Posouzení vlivu na ochranu osobních údajů

- Popis zamýšlených operací
- Posouzení nezbytnosti a přiměřenosti
- Posouzení rizik
- Opatření k řešení těchto rizik

DPIA: předchozí konzultace



Hlášení porušení

- Došlo k porušení zabezpečení?
- Dotýká se porušení osobních údajů?
- Jsou s tímto porušením spojeny rizika pro práva a svobody FO?
- Jsou tato rizika vysoká?

Hlášení porušení ÚOOÚ

- Co se stalo
- Čeho se porušení dotklo
- Jméno a kontaktní údaje pověřence nebo jiného kontaktního místa
- Popis pravděpodobných důsledků

Úkol 5

6. Pověřenec pro ochranu osobních údajů

Kdo musí mít pověření?

1. Orgán veřejné moci nebo veřejný subjekt
2. Rozsáhlé a pravidelné monitorování
3. Rozsáhlé zpracování zvláštní kategorie údajů

Co musí splňovat pověřenec?

1. Nezávislost
2. Nestrannost

Co má splňovat pověřenec?

1. Znalost práva na ochranu osobních údajů
2. Znalost IT
3. Znalost interních procesů organizace

Interní pověřenec

1. Může být zaměstnanec nezávislý? Který zaměstnanec?
2. Odpovědnost za škodu?
3. Pracovní zařazení?

Externí pověřenec

1. Zná interní procesy organizace?
2. Zná prostředí lékáren?
3. Je nezávislý?

IV. Co dělá pověřenec?

1. Poskytuje poradenství o zpracování
2. Monitoruje soulad s GDPR
3. Spolupracuje s ÚOOÚ
4. Kontaktní místo pro ÚOOÚ
5. Vyřizuje stížnosti

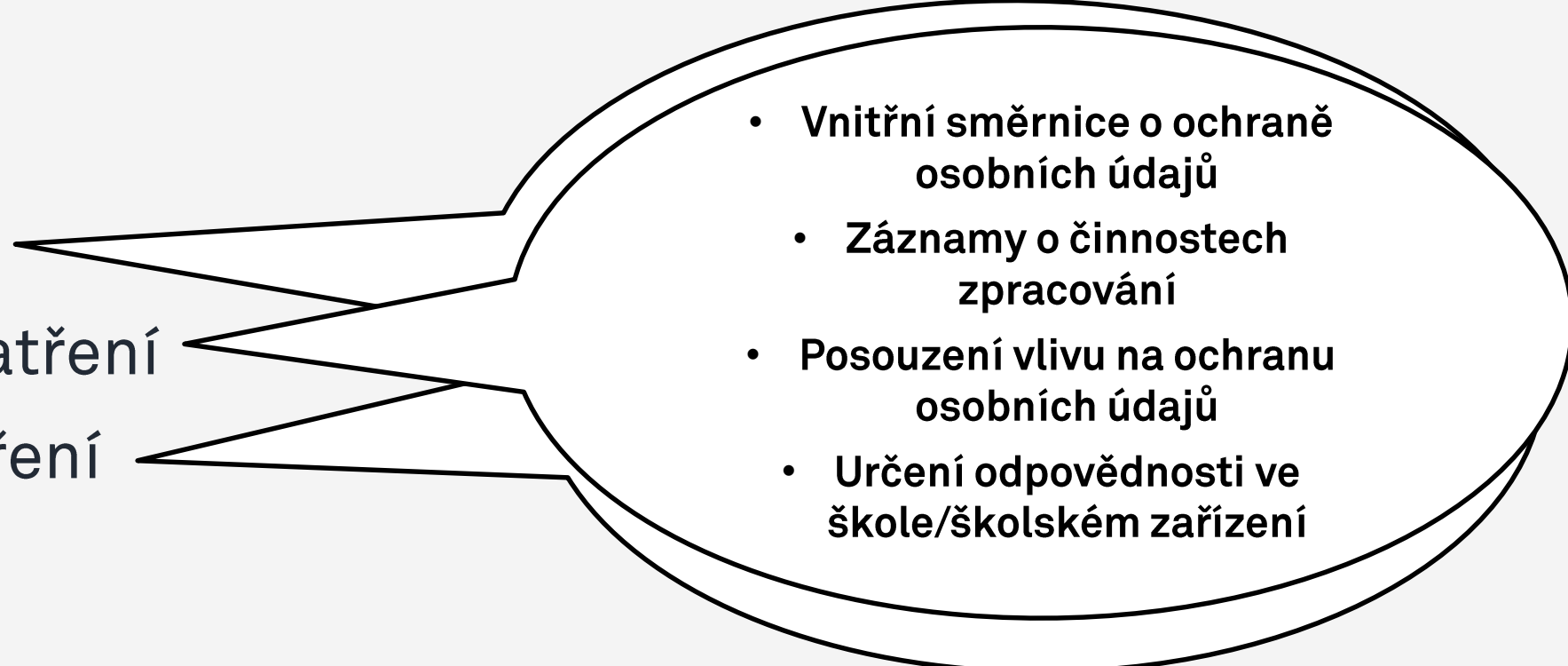
7. Shrnutí

I. Zajištění souladu s GDPR:

1. Mapování
2. Vyhodnocení
3. Přijetí opatření

II. Zajištění souladu s GDPR:

1. Právní opatření
2. Organizační opatření
3. Technická opatření

- 
- Vnitřní směrnice o ochraně osobních údajů
 - Záznamy o činnostech zpracování
 - Posouzení vlivu na ochranu osobních údajů
 - Určení odpovědnosti ve škole/školském zařízení

Jak začít?



3 kroky k GDPR minimu:

1

Interní směrnice

2

Záznamy o činnostech zpracování

3

Školení
zaměstnanců



Jak Vám můžeme zjednodušit život?

1

**12 kroků k implementaci
v PDF mailem**

2

Příprava dokumentace

3

Vstupní analýza



Děkuji za pozornost

Alice Frýbová

alice.frybova@holubova.cz