



# GDPR

## VE VZTAHU K LÉKÁRENSKÉ PRAXI

Mgr. Martin Dymáček, LL. M., advokát

7.4.2018, Kurdějov

# Co, kdy a proč se mění?

- **nyní zákon č. 101/2000 Sb., o ochraně osobních údajů**
  - účinný již od 1.6.2000
- **nově nařízení č. 2016/679/EU, obecné nařízení o ochraně osobních údajů (GDPR)**
  - účinnost od 25.5.2018
- proč ke změně dochází:
  - pouze nepřímá aplikovatelnost původní směrnice 95/46/ES
  - velké rozdíly mezi členskými státy
  - snaha o sjednocení právní úpravy v celé EU

# Podstata změn

- žádná revoluce, ale evoluce právní úpravy
- stejná práva a povinnosti napříč EU
  - výhoda pro koncerny, na lokální správce nemá vliv
- posílení práv subjektů údajů
  - právo na přenositelnost osobních údajů
  - právo na omezení zpracování
  - právo nebýt předmětem automatizovaného individuálního rozhodování
- posílení povinností správců/zpracovatelů
  - povinnost provádět posouzení vlivu
  - předchozí konzultace s dozorovým úřadem
  - povinnost jmenovat pověřence ve stanovených případech

# Co se naopak nemění?

- základní **pojmy**
- povinnost mít pro každé zpracování **řádný titul**
- povinnost **minimalizace** zpracování osobních údajů
- povinnost zpracování jen pro **konkrétní účely**
- povinnost mít zpracování upraveno v **interních předpisech**
- povinnost mít zpracování osobních údajů 3. subjektem ošetřeno **písemnou smlouvou**
- povinnost vést **záznamy o činnostech**
- **administrativní zátěž**
- **málo kontrolorů**

# Základní pojmy

- osobní údaj
- zvláštní kategorie osobních údajů (citlivý údaj)
- subjekt údajů
- zpracování osobních údajů
- správce osobních údajů (společní správci)
- zpracovatel osobních údajů
- příjemce osobních údajů
- profilování
- anonymizace
- pseudonymizace

# Zásady zpracování osobních údajů

- zákonnost, korektnost a transparentnost
- shromažďování jen pro určité, výslovně vyjádřené a legitimní účely
- minimalizace údajů
- přesnost údajů
- (časové) omezení uložení
- náležité zabezpečení zpracování
- povinnost správce být schopen doložit soulad

# Zákonné důvody zpracování OÚ

Obecně	Citlivé údaje
plnění smlouvy (jednání před jejím uzavřením)	
plnění právní povinnosti správce	plnění povinnosti a výkon práv správce a SÚ v oblasti pracovního práva a soc. zabezpečení, pokud povoleno právem EU/ČS
ochrana životně důležitých zájmů subjektu údajů/jiné FO	jen v případě, že SÚ není fyzicky nebo právně způsobilý udělit souhlas
plnění úkolů ve veřejném zájmu/při výkonu veřejné moci správcem	<ul style="list-style-type: none"><li>- pouze neziskový subjekt v rámci své oprávněné činnosti, vhodné záruky, členové</li><li>- nezbytnost z důvodu významného veřejného zájmu na základě práva EU/ČS</li><li>- nezbytnost pro poskytování zdravotní nebo sociální péče či léčby, lékařské diagnostiky apod.</li><li>- nezbytnost z důvodu veřejného zájmu v oblasti veřejného zdraví (zajištění přísných norem kvality a bezpečnosti LP a ZP apod.)</li><li>- nezbytnost pro účely archivace ve veř. zájmu</li></ul>
výkon oprávněných zájmů správce/3. strany	nezbytnost pro určení, výkon, obhajobu právních nároků
souhlas subjektu údajů	výslovný souhlas subjektu údajů pokud byly zjevně zveřejněny subjektem údajů

# II. část - Příprava na GDPR

## KROK ZA KROKEM



# Posouzení vlivu

- musí **předcházet** zahájení zpracování
- netýká se obecně všech správců
- pouze pokud je pravděpodobné, že určitý druh zpracování bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek **vysoké riziko pro práva a svobody FO**
- nutné zejména v případě **rozsáhlého zpracování citlivých údajů** (o zdravotním stavu)
- podle čl. 35 odst. 10 GDPR a návrhu prováděcího zákona **neplatí pro činnosti uložené zákonem**
- **obdobné otázky je však stejně nucen každý správce řešit vždy:**  
*co, o kom, za jakým účelem, jak dlouho zpracovává, jaké operace, je to nezbytné a přiměřené účelům, posouzení rizik, plánovaná opatření k jejich řešení*

# Posouzení vlivu - příklad

	Pacienti		Zaměstnanci		Obchodní partneři	
Kategorie zpracovávaných OÚ	jméno, příjmení, r.č., adresa, telefon, údaje o zdravotním stavu (...)		jméno, příjmení, r.č., bydliště, telefonní číslo, e-mail, ...		jméno, příjmení, IČ, DIČ, sídlo, telefon, e-mail, ...	
Účely a zákonné důvody zpracování	Účel	Důvod	Účel	Důvod	Účel	Důvod
	Poskytování zdravotních služeb	plnění smlouvy nezbytnost pro poskytování zdravotní péče	plnění povinností zaměstnavatele	plnění smlouvy plnění právní povinnosti	vedení databáze partnerů	plnění smlouvy oprávněný zájem
	vypořádání nároků z veř. zdravotního pojištění	plnění smlouvy nezbytnost pro poskytování zdravotní péče			marketing	souhlas
	vedení klientské databáze	plnění smlouvy souhlas (jde-li zpracování nad rámec smlouvy) apod.				
Popis zamýšlených operací	<ul style="list-style-type: none"> <li>- sběr OÚ přímo od pacientů</li> <li>- vložení OÚ do databáze</li> <li>- předávání OÚ 3. subjektům (pojišťovna, účetní, IT poskytovatel apod.)</li> </ul>					
Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů zpracování						
Posouzení rizik pro práva a svobody SÚ						
Plánovaná opatření k řešení rizik (bezpečnostní opatření)	<ul style="list-style-type: none"> <li>- fyzické zabezpečení prostor zpracování (uzamčení)</li> <li>- antivirové programy</li> <li>- přístupová práva, pravidelně obměňovaná hesla</li> </ul>					

# Předchozí konzultace

- konzultace s Úřadem pro ochranu osobních údajů
- pokud z posouzení vlivu vyplývá, že dané zpracování by mělo za následek **vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění** tohoto rizika
- stále musí předcházet zahájení zpracování
- ÚOOÚ zareaguje do 8 týdnů
- není nijak specifikováno, na co se bude vztahovat
- **diskutabilní** – ustanovení je zcela blanketní, udávám se předem, pokud neprovedu opatření, vůbec nesmím zpracovávat

# Záznamy o činnostech

- povinnost vést je má každý správce a zpracovatel, ledaže jde o podnik do 250 osob
- v případě zpracovávání citlivých údajů ale povinnost platí bez dalšího
- vedou se písemně či elektronicky
- musí být poskytnuty na požádání ÚOOÚ – nejen v případě kontroly

# Záznamy o činnostech

- obsahují:
  - jméno a kontaktní údaje správce, zástupce, pověřence
  - účely zpracování
  - kategorie subjektů údajů (zaměstnanci, pacienti)
  - kategorie osobních údajů (jméno, příjmení, adresa, ...)
  - kategorie příjemců (subdodavatelé)
  - informace o případném předání do 3. země
  - plánované lhůty pro výmaz jednotlivých kategorií údajů
  - obecný popis užívaných technických a organizačních bezpečnostních opatření

# Pověřenec pro ochranu osobních údajů

- nemá povinnost jmenovat jej každý správce a zpracovatel
- povinnost jmenovat, pokud hlavní činnosti správce spočívají v rozsáhlém zpracování citlivých údajů – kritéria:
  - počet dotčených subjektů (absolutně x podíl příslušné skupiny)
  - objem zpracovávaných údajů
  - trvání nebo stálost činnosti zpracovávání
  - zeměpisný rozsah zpracování
- skupina podniků může jmenovat jediného
- povinnosti:
  - poskytování informací a poradenství správcům a zpracovatelům o jejich povinnostech
  - monitorování souladu s GDPR a s předpisy správce
  - spolupráce s dozorovým úřadem – plní oznamovací povinnosti (i proti vůli správce)
  - kontaktní místo pro dozorový úřad

# Pověřenec pro ochranu osobních údajů

- může být zaměstnanec i OSVČ
  - problém: nesmí dostávat žádné pokyny týkající se jeho úkolů
  - problém: nesmí být propuštěn ani sankcionován za plnění úkolů pověřence
  - přímo podřízen vrcholovým pracovníkům
  - může vykonávat i jiné úkoly a povinnosti x střet zájmů
- kritéria:
  - profesní kvality
  - odborné znalosti práva
  - praxe v oblasti ochrany údajů
  - zároveň ne advokát
  - kde brát?

# Postup při přípravě na GDPR

- **interní „posouzení vlivu“ – vnitřní audit**
  - co, o kom, proč, na jak dlouho a jak zpracovávám, komu údaje předávám
  - rozdělit dle kategorií údajů (zaměstnanci, pacienti, obchodní partneři)
  - nezapomenout na kamerové a docházkové systémy apod.
- **zhodnocení zjištěného stavu**
  - platnost titulů, zejm. souhlasů, obsah užívaných smluv
  - technická připravenost na GDPR (neprodlený výmaz a přenos OÚ, sledování přístupů do databáze, antivirové zabezpečení apod.)
  - protřídění rozsahu údajů dle účelů zpracování i účelů samotných (č. OP)
  - rozdělení odpovědnosti mezi zaměstnance
- **příprava interních předpisů a záznamů o činnosti**
  - stanovit jasná pravidla a odpovědnost zaměstnanců za oblast zpracování osobních údajů
  - ochrana zaměstnavatele pro případ pochybení zaměstnanců
  - seznámení zaměstnanců s jejich obsahem, pravidelná školení



# Postup při přípravě na GDPR

- **nalezení a jmenování pověřence**
  - pokud z „posouzení vlivu“ vyjde najevo rozsáhlé zpracovávání citlivých údajů
  - pozor na „výhodné“ nabídky „certifikovaných“ osob
- **aktualizace souhlasů, poučení o právech, OP**
- **uzavření smluv/dodatků ke smlouvám se zpracovatelem**
  - náležitosti dle čl. 28 odst. 3 GDPR
  - nutná písemná forma
  - např. externí účetní – kdokoli, kdo není zaměstnanec správce
- **pravidelné vedení a aktualizace záznamů o činnosti**
- **pravidelné školení odpovědných osob**

# Děkuji za pozornost

Mgr. Martin Dymáček, LL. M., advokát

[dymacek@dymaceklegal.cz](mailto:dymacek@dymaceklegal.cz)

+ 420 735 800 088

JUDr. Alena Šildová, advokátka

[sildova@dymaceklegal.cz](mailto:sildova@dymaceklegal.cz)

+420 777 994 874