# Příprava IS na příchod GDPR

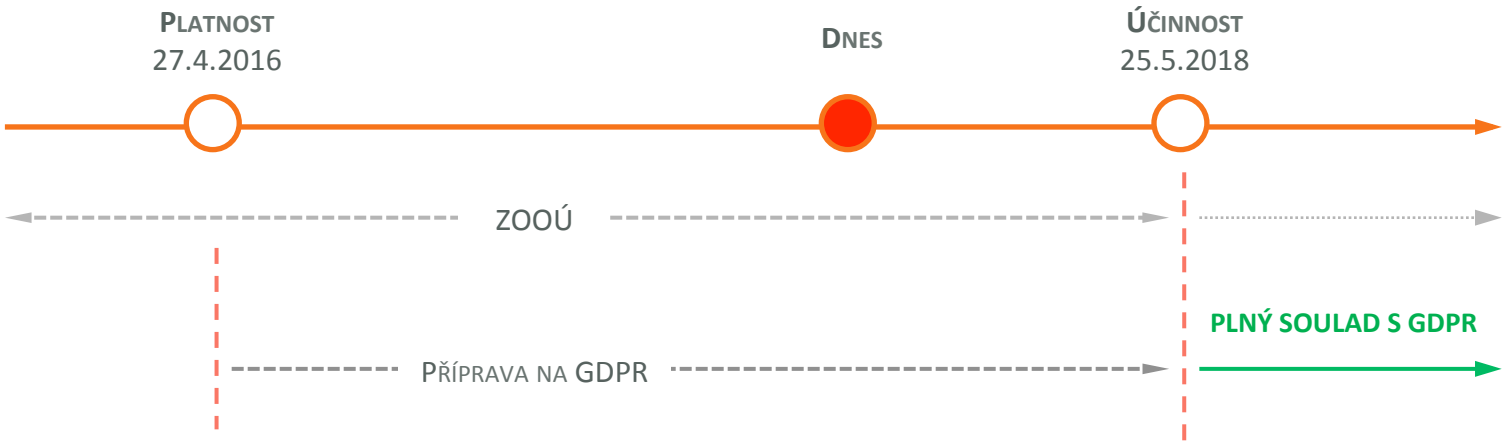
## se zaměřením na ISP

Jan Zahradníček
AK Velíšek & Podpěra

# KDY TO NASTANE?

GDPR = GENERAL DATA PROTECTION REGULATION

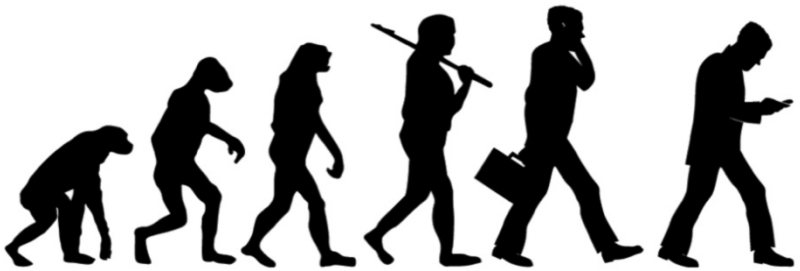
Nařízení Evropského parlamentu a Rady (EU) 2016/679 - obecné nařízení o ochraně osobních údajů




Velíšek & Podpěra
advokátní kancelář s.r.o.

REVOLUCE …

… NEBO EVOLUCE ?



Velíšek & Podpěra
advokátní kancelář s.r.o.

# VĚTŠINA POVINNOSTÍ PLATÍ JIŽ NYNÍ !!!

**zákon o ochrane osobných údajov** (122/2013 Zb.)

- stanovit účel zpracování, provádět zpracování pouze v rozsahu, který odpovídá stanovenému účelu
- zpracování pouze na základě zákonného důvodu (zákon, souhlas, plnění smlouvy …)
- povinnost zabezpečit osobní údaje před neoprávněným přístupem, ztrátou, zneužitím
- informační povinnost ve vztahu k subjektu údajů
- povinnost přijmout technická, organizační a personální opatření k zajištění ochrany

**zákon o elektronických komunikáciách** (351/2011 Zb.)

- § 56 ZoEK - ochrana osobních údajů
  - technická a organizační opatření k zajištění bezpečnosti poskytovaných služeb – s ohledem na dostupný stav techniky, náklady a přiměřeně existujícímu riziku
  - povinnost hlásit incidenty
- § 57 ZoEK provozní a lokalizační údaje
  - opět povinnost zabezpečit před neoprávněným přístupem, ztrátou zničením
  - pouze v rozsahu stanoveném v zákoně, jinak pouze se souhlasem subjektu údajů

Velíšek & Podpěra advokátní kancelář s.r.o.

# CO GDPR POŽADUJE?

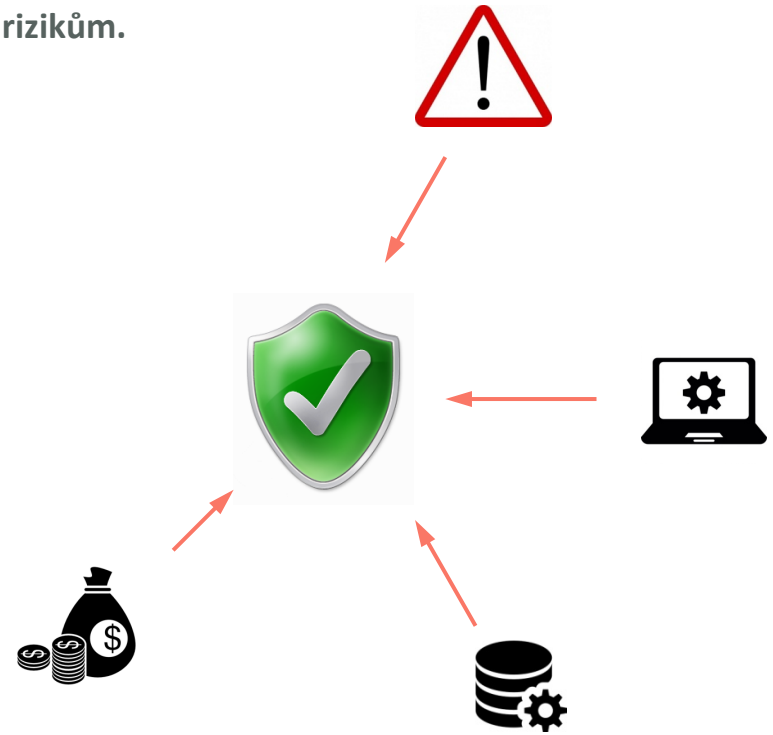
Správce a zpracovatel jsou povinni provést vhodná

- **technická opatření** a
- **organizační opatření**

aby zajistili úroveň zabezpečení, **která odpovídá možným rizikům.**

Přitom je potřeba zohlednit

- stav techniky a dostupné technologie
- náklady na implementaci
- povahu, rozsah a účel zpracování
- pravděpodobná rizika a jejich závažnost



Velíšek & Podpěra advokátní kancelář s.r.o.

# PŘÍPRAVA IS NA GDPR

**IS jako takové již mohou být na GDPR dostatečně připraveny**

- IS jsou zabezpečeny, reflektují aktuální stav techniky a technologií
- vendoři a poskytovatelé služeb deklarují GDPR ready / GDPR compliant stav

**Problém může být naopak v práci s IS**:

- v tom, jaká data jsou v IS ukládána
- aktuálnost dat, duplicity
- přístup k datům
- způsobu práce s daty
- předávání 3. stranám


Velíšek & Podpěra advokátní kancelář s.r.o.

# ZÁSADY NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI V IS

- OMEZENÍ ÚČELEM ZPRACOVÁNÍ A MINIMALIZACE ROZSAHU ZPRACOVÁNÍ
  - pouze osobní údaje, které jsou nezbytné pro poskytování služeb , zpracování příslušné agendy nebo plnění právních povinností (data retention)
  - shromažďovány údaje v příliš širokém rozsahu, příp. bez potřebného právního důvodu
- OMEZENÍ DOBY ULOŽENÍ
  - údaje, u kterých odpadnul důvod zpracování, musí být vymazány
- PŘESNOST
  - zpracovávat pouze aktuální osobní údaje
  - odstranění duplicit a nepřesností
- INTEGRITA A DŮVĚRNOST
  - bezpečnost zpracování, bezpečnost IS
  - zamezení neoprávněného přístupu k datům
  - ochrana před zneužitím, ztrátou nebo zničením

Velíšek & Podpěra advokátní kancelář s.r.o.

# CO ZOHLEDNIT V PRAXI

- řízení přístupů k datům jako takovým a k různým skupinám dat
  - technik nemusí mít přístup k údajům o bankovních účtech klienta
  - operátor call centra nemusí znát údaje o zaměstnancích
  - personalista nemusí znát údaje o klientech
- oddělení osobních údajů získaných k různým účelům
  - pro jednotlivé agendy samostatné /oddělené databáze – v jejich rámci nastavit příslušná přístupová oprávnění
- práce s osobními údaji v různých podobách
  - osobní údaje mohou být z IS exportovány do papírové podoby
  - ochrana se vztahuje i na manuální zpracování (archiv, kartotéka)
- zabezpečení koncových zařízení a zásady práce s koncovým zařízením
  - zranitelnost skrze uživatelské stanice
  - ukládání na lokální úložiště
- zvýšit povědomí o možných rizicích

Velíšek & Podpěra advokátní kancelář s.r.o.

# JAK SE TEDY NA GDPR PŘIPRAVIT?

VĚDĚT, JAKÉ OSOBNÍ ÚDAJE ZPRACOVÁVÁM, K JAKÉMU ÚČELU, NA ZÁKLADĚ JAKÉHO TITULU, JAK DLOUHO, KOMU PŘEDÁVÁM – ANALÝZA OÚ

ZMAPOVAT, V JAKÝCH IS JSOU OÚ ULOŽENY, V JAKÉ PODOBĚ, KDO K NIM MÁ PŘÍSTUP, JAK JSOU ZABEZPEČENY – TECHNICKÁ A PROCESNÍ ANALÝZA

ZNÁT POVINNOSTI, KTERÉ SE NA SPRÁVCE VZTAHUJÍ – PRÁVNÍ POVĚDOMÍ

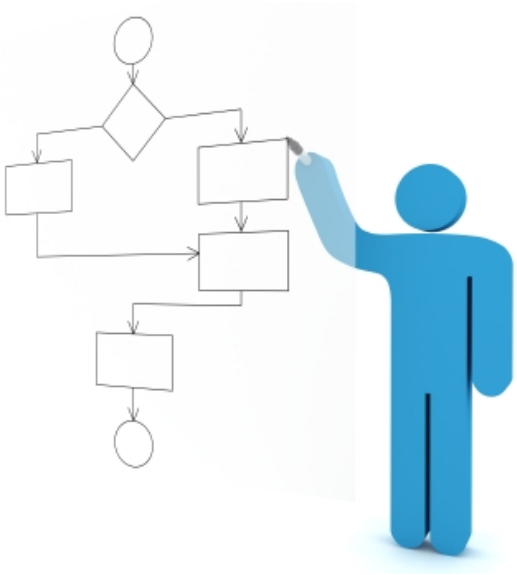
REVIZE STÁVAJÍCÍ DOKUMENTACE – SMLOUVY, VOP, INTERNÍ PŘEDPISY

Velíšek & Podpěra
advokátní kancelář s.r.o.

# Doporučený postup

Příprava na GPDR by měla zahrnovat následující kroky

1. Vstupní analýza – analýza současného stavu zpracování a bezpečnosti
2. Srovnávací analýza – identifikace nedostatků
3. Identifikace vhodných řešení k dosažení shody
4. Implementace řešení
5. **Plný soulad s GDPR**



Velíšek & Podpěra advokátní kancelář s.r.o.

# Závěr

GDPR je komplexní problém, který nevyřeší nový SW nástroj, interní směrnice nebo školení

S přípravou na GDPR je potřeba začít co nejdříve

Je potřeba zapojit celou firmu – dopad do řady oblastí (IT, personalistika, správa klientů, back office…)

Přijmout ochranu osobních dat a ochranu soukromí jako součást firemní kultury

Velíšek & Podpěra advokátní kancelář s.r.o.

# Děkuji za pozornost

Jan Zahradníček
e-mail: zahradnicek@akpv.cz

Velíšek & Podpěra - advokátní kancelář s.r.o.
Holečkova 105/6, 150 00 Praha 5
www.akpv.cz