



# GDPR

## Aneb co se nedá stihnout

e-government 20:10, Mikulov, 5. – 6. 9. 2017  
včas

Mgr. Michal Nulíček, LL.M.  
ROWAN LEGAL

# Plán prezentace



## ■ Dopady GDPR

GDPR a veřejná správa - co čekat a na co se připravit?

## ■ Pomůže vnitrostátní úprava?

Novela ZOOÚ je v připomínkovém řízení - přináší úlevu?

## ■ Co učinit nyní a kde se dozvědět více?

Zbývá posledních měsíců, co je třeba udělat, aby nedošlo na pokuty?

# GDPR a veřejná správa

Co čekat a na co se připravit?



## ZPŘÍSNĚNÍ SANKCÍ



Lze očekávat, že ÚOOÚ již veřejné správě nebude ukládat zanedbatelně nízké sankce

## ŽÁDOSTI SUBJEKTŮ



Očekáváme výrazný nárůst žádostí o výkon práv

## NOVÉ POVINNOSTI



Záznamy, prokazování souladu, bezpečnost, pověřenec, incidenty, DPIA

Dopady se uplatní jak při zpracování **navenek** (výkon veřejné správy), tak **uvnitř** (při zpracování údajů zaměstnanců)

# Co GDPR přináší? I.

Využívejte osobní údaje podle pravidel



## Zákonnost

Vyplývají všechna zpracování v plném rozsahu ze zákona či jiného titulu? **STANOVTE A OVĚŘUJTE**

## Omezení účelem

K čemu osobní údaje potřebujete? Jak je plánujete využívat?

→ **URČETE ÚČEL PŘEDEM** (údaje pro odlišné účely oddělit)

## Minimalizace

Nezpracováváte údaje ve větším než nezbytném rozsahu?

Neuchováváte je po delší než nutnou dobu?

→ **KONTROLUJTE, OMEZTE A MAŽTE**

# Co GDPR přináší? II.

## Využívejte osobní údaje podle pravidel



### Transparentnost

Informujete subjekty údajů o zpracování? Novinky: více informací, srozumitelnější jazyk, vrstvení informací

→ **AKTUALIZUJTE**

### Integrita a důvěrnost

Chráníte dostatečně osobní údaje? Víte, co dělat v případě narušení?

→ **ZABEZPEČTE A HLAŠTE**

### Odpovědnost

→ **DODRŽUJTE, DOKUMENTUJTE A PROKAZUJTE**

# Co GDPR přináší? III.

**Nepodceňujte bezpečnostní rizika, vhodná opatření začleňte do každého procesu**



## Privacy by design

Určete při návrhu zpracování a při zpracování samotném opatření ochrany přiměřená stavu techniky, nákladům na provedení, povaze a riziku zpracování.

## Privacy by default

Zajistěte, že budou zpracovávány nezbytné údaje, po nezbytnou dobu, s přístupem pouze určených osob.

## Compliance systém

Definujte politiku ochrany, procesy, povinnosti pracovníků a jejich splnění monitorovat a hodnotit.

## Zabezpečení zpracování

Přijměte vhodná opatření ochrany přiměřená stavu techniky, nákladům na provedení, povaze a riziku zpracování.

# Co GDPR přináší? IV.

## Práva subjektů přinášejí nové povinnosti správcům a zpracovatelům



### Zpracovatelé

Vyberte důvěryhodné zpracovatele, uzavřete smlouvy s nezbytnými náležitostmi a kontrolujte zpracování.

### DPIA

Proveďte posouzení vlivu u rizikových zpracování, v případě vysokého rizika konzultujte s ÚOOÚ.

### DPO

Zajistěte nezávislého a kvalifikovaného pověřence pro ochranu os. úd.

### Incidenty

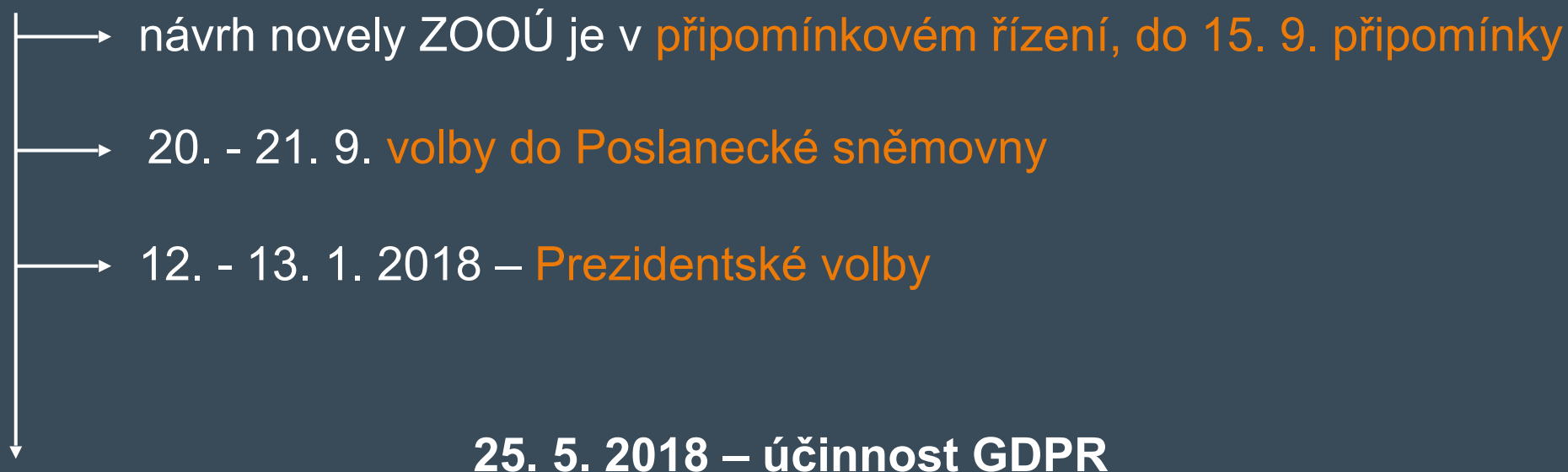
Monitorujte, evidujte a ohlašujte rizikové incidenty ÚOOÚ a vysoce rizikové incidenty subjektům údajů.



**Snížení rizikovosti incidentů, omezení případů povinných oznámení incidentů, snížení či vyloučení škody**

# Novela „stojedničky“

## Legislativní proces v plném proudu – stihne se do účinnosti GDPR?



Účinnost **nejistá**



# GDPR a český zákon I.

## Co novela upravuje a co se nevešlo?



- ! Novela ZOOÚ může být velmi vhodným způsobem, jak **omezit některé povinnosti dopadající na veřejnou správu**, očekáváme však že ještě budou provedeny dílčí úpravy a zpřesnění novely a specifické záležitosti upraveny v sektorové legislativě (zdravotnictví, finanční služby apod.).

### § 4 novely ZOOÚ

Oprávnění ke zpracování údajů na základě povinnosti či veřejného zájmu



### § 5 novely ZOOÚ

Stanoví **obecnou slučitelnost účelů**, otázkou je konkrétnost ve smyslu čl. 6/4 GDPR



# GDPR a český zákon II.

## Co novela upravuje a co se nevešlo?



### §§ 7, 8, 10, 11 novely ZOOÚ

Stanoví **výjimky z práv a povinností dle čl. 12-22 GDPR**, i zde je otázkou konkrétnost ve smyslu čl. 23 GDPR



### Požadavky GDPR na výjimky v čl. 23 jsou následující:

- **Konkrétní** legislativní opatření pro konkrétní případy.
- Odůvodněnost některým ze **sledovaných veřejných zájmů** (národní bezpečnost, obrana, nezávislost soudnictví apod.).
- **Vymezení** účelů zpracování, zpracovávaných údajů, rozsahu omezení, záruk proti zneužití, specifikace správců, doby uložení, rizik pro subjekty a právo na informování o omezení.

# GDPR a český zákon III.

## Co novela upravuje a co se nevešlo?



### § 9 novely ZOOÚ

Vylučuje povinnost dle čl. 35 GDPR, užívá však mírně odlišný přístup než předpokládá čl. 23 a čl. 35 odst. 10 GDPR



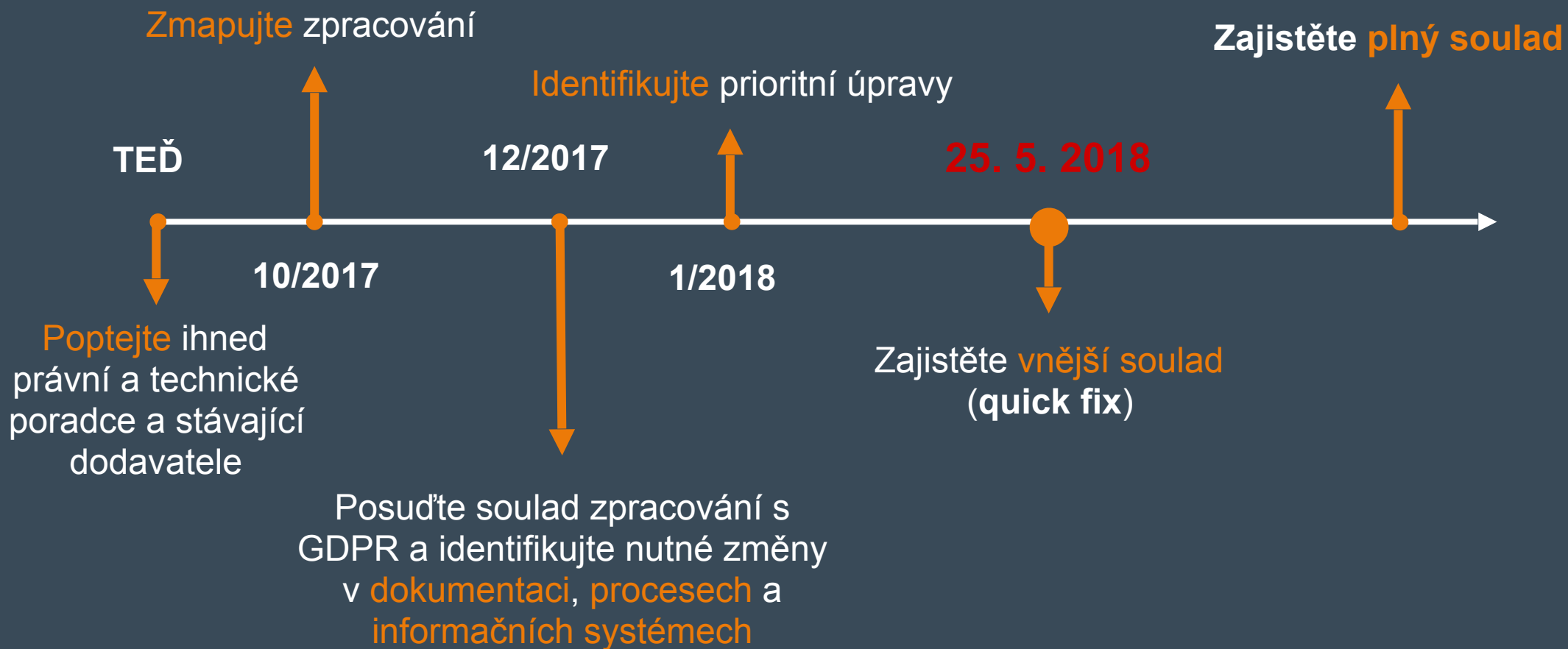
**Čl. 23 neumožňuje omezení povinností dle čl. 35 a současně čl. 35 odst. 10 umožňuje neprovést DPIA jen tehdy, pokud:**

- zpracování má základ v zákoně; a současně
- v legislativním procesu bylo provedeno DPIA (dosud nebylo provedeno u žádného zákona).

# Krizový harmonogram implementace



Nastavte si priority, aneb zbývá posledních pár měsíců



# Quick fix GDPR

## Zkratka k GDPR

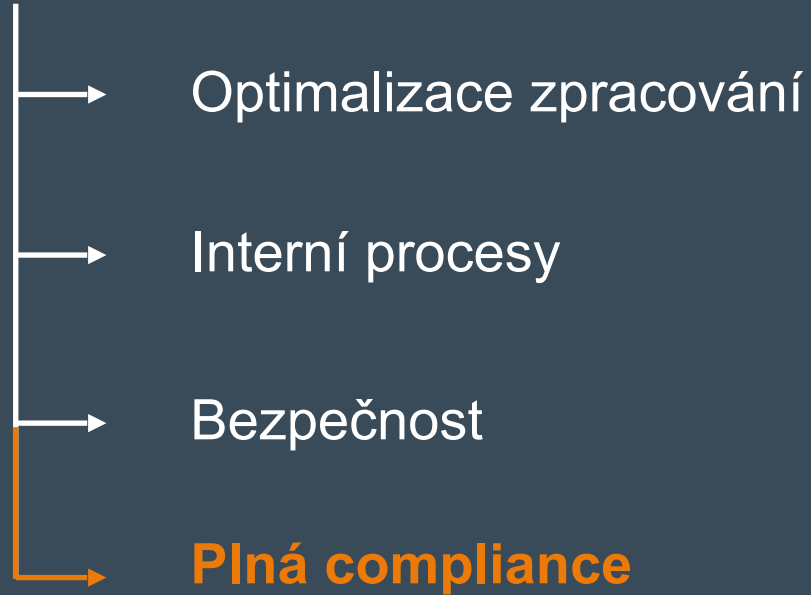


- Vnější dokumentace a DPO
- Umožnění výkonu práv
- Zpracovatelské smlouvy
- **Vnější compliance**



# Implementace GDPR jako projekt

## Dosáhněte plného souladu s GDPR



# Co si odnést?



**Čas se krátí, s přípravou je třeba začít hned!**

- GDPR má **zásadní dopady** na veřejnou správu
- Novela ZOOÚ **neznamenaá vynětí VS z působnosti GDPR** a nelze na ni plně spoléhat
- Bude nutno upravit **dokumentaci, procesy a informační systémy**, zavést **technická a organizační opatření** ochrany, jmenovat **DPO**
- **Při okamžitém zahájení lze quick fix stihnout do účinnosti GDPR**

# Co umíme a jak můžeme pomoci?



Školení



Certifikace

**DPO**



jako  
**SLUŽBA**



Právní  
poradenství



# Kde se můžete o GDPR dozvědět víc?



[www.GDPRcompliance.eu](http://www.GDPRcompliance.eu)

LinkedIn – [ROWAN LEGAL](#) nebo [GDPR Compliance](#)

Nebo si napište o newsletter – [nulicek@rowanlegal.com](mailto:nulicek@rowanlegal.com)



První komentář k GDPR v ČR  
V prodeji na: [www.wolterskluwer.cz](http://www.wolterskluwer.cz)

**Sleva 15 %**  
při využití kódu  
**GDPR062017**



## Děkujeme za pozornost

Mgr. Michal Nulíček, LL.M.  
*nulicek@rowanlegal.com*

**ROWAN LEGAL**

+420 224 216 212

[www.rowanlegal.com](http://www.rowanlegal.com)

- Právnícká firma roku v kategorii Právo informačních technologií  
- V letech 2010, 2011, 2012, 2013, 2014, 2015 a 2016
- Band 1 v oblasti TMT pro Českou republiku dle Chambers & Partners

# Pověřenec pro ochranu údajů

## Samostatný nebo společný pověřenec?



### Samostatný pověřenec

Jeden pověřenec pro každou organizaci

- V místě zpracování
- Jednodušší monitorování souladu a analýza podkladů
- Odlišnosti v přístupu k ochraně
- Větší požadavky na lidské zdroje-> vyšší náklady
- Nižší úroveň specializace
- Vyšší riziko střetu zájmů



### Společný pověřenec

Jeden pověřenec pro více organizací

- Jednotnost dokumentace a procesů
- Jednotné kontaktní místo pro dozorový úřad
- Vyšší míra součinnosti ostatních správců a zpracovatelů ve skupině

# Pověřenec pro ochranu údajů

## Interní nebo externí pověřenec?



Povinnost správce a zpracovatele zajistit, že nebude docházet ke střetu zájmů

### Interní

- Lepší dostupnost
- Vhled do procesů
- Potenciálně nižší náklady

- Investice do vzdělávání
- Změna pověřence
- Odpovědnost a náhrada škody
- Vyšší riziko střetu zájmů

### Externí

- Změna pověřence
- Investice do vzdělávání
- Odpovědnost a náhrada
- Střet zájmů

- Přejícné období
- Exkluzivita správce