# Obecné nařízení o ochraně osobních údajů

předpis, který nahradí zákon o ochraně osobních údajů

# GDPR

účinnost v květnu 2018

náhrada směrnice 95/46/ES

regulace ochrany osobních údajů pro 21. století

reakce na nové technologie

revoluce i evoluce

# Stav GDPR v ČR

pracovní skupina - ÚV

legislativní práce - MV a další(?)

novela zákona č. 101/2000 Sb., a dalších(?)

- odborné skupiny
- profesními sdružení
- průmyslové svazy

# Evoluce ochrany údajů v ČR

zákon č. 256/1992 Sb.

zákon č. 101/2000 Sb.

- novela 2004
- novela 2007

zabezpečení, citlivá biometrika

data breaches v zákonu č. 127/2005 Sb.

# GDPR ve zkratce

kontinuita s 95/ES/46

principy ochrany – zpřesněné až rozšířené

základní pojmy - bez zásadních změn

práva subjektů – podrobnější

povinnosti správců a zpracovatelů - rozšířené

nové nástroje ochrany údajů

celoevropský dozor

# Působnost GDPR

správce, zpracovatel

zpracování údajů / nabízení služeb či zboží v EU

osobní údaje na internetu

pseudonymizované údaje

Výjimky:

- národní bezpečnost, law enforcement
- osobní potřeba

# Staronové principy GDPR

zákonnost

férovost

přiměřenost / omezení účelem

minimalizace údajů

přesnost

odpovědnost

transparentnost

# Nové principy GDPR

accountability

RBA / risk based assessment

privacy by design

privacy by default

# Práva lidí dotčených zpracováním

být informován
mít přístup
uplatnit námitky

žádat

- opravu
- výmaz
- omezení
- přenesení údajů

# Jak komunikovat s lidmi

vysvětlit zpracování

umožnit přístup k údajům / přenositelnost

varovat při narušení bezpečnosti

nadstandardně chránit citlivé údaje

mít vyřešeno - výmaz údajů, profilování, souhlas, marketing, přenos dat mimo EU

# Podpora důvěry ve zpracování

accountability

proaktivní opatření – by design & by default

RBA

vylepšování bezpečnostních prvků

pseudonymizace údajů

minimalizace zpracování údajů

# Pseudonymizace

zpracování takovým způsobem, že osobní údaje již nemohou být přiřazeny konkrétnímu subjektu bez dodatečných informací

záruka zpracování, snižuje rizika

„změkčuje“ povinnosti správců

dodatečné informace

- uchovávat odděleně
- zajistit, aby nebyly přiřazeny identifikované či identifikovatelné osobě

# Záměrná a standardní ochrana údajů

aplikace zásad ochrany údajů účinným způsobem

posuzovat vliv jednotlivých zpracování

začlenit do zpracování potřebné záruky

přihlížet k řadě faktorů

- účel, povaha, kontext, rozsah zpracování
- stav techniky
- náklady na provedení

# Nové nástroje (a RBA!)

zabezpečení zpracování - čl. 32

ohlášení a oznámení porušení zabezpečení - čl. 33 a 34

záznamy o činnostech zpracování - čl. 30

posuzování vlivu - čl. 35

předchozí konzultace - čl. 36

pověřenec pro ochranu osobních údajů - čl. 37

# Zabezpečení

Schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování.

Schopnost obnovit dostupnost osobních údajů a přístup k nim v případě technických či fyzických incidentů.

Proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

# Zabezpečení (2)

umožňuje zohlednit stav techniky, náklady na provedení, kontext, účel

nová ohlašovací povinnost a oznamovací povinnost

detailnější a pružnější ve srovnání s § 13 zákona č. 101/2000 Sb.

návod na vhodnou úroveň bezpečnosti

# Data breaches

každý případ s riziky pro práva dotčených lidí ohlásit dozorovému úřadu, pokud možno do 72 hodin

u vysokého rizika také oznámit dotčeným (ohroženým) lidem

oznámení se nevyžaduje, pokud

- ochranná opatření činí údaje pro neoprávněné osoby nesrozumitelnými
- následná opatření eliminují rizika
- by oznámení vyžadovalo nepřiměřené úsilí

# Posouzení vlivu

povinné vždy pro zpracování

- systematické a rozsáhlé, zahrnující vyhodnocování osobních aspektů, automatizovaná rozhodování, profilování, coby základ pro rozhodování s pr. účinky
- zvláštních kategorií  údajů
- zahrnující systematické monitorování veřejně přístupných prostor

# Záznamy o činnostech zpracování

pro riziková zpracování

pro zpracování citlivých údajů

pro podniky s 250 a více zaměstnanci

správce na požádání poskytne dozorovému úřadu

# Pověřenec pro ochranu osobních údajů

povinný pro zpracování

- prováděná orgány veřejné moci či veřejnými subjekty
- rozsáhlá a závažná zpracování zahrnující pravidelné a systematické monitorování lidí
- zvláštních kategorií údajů

# Konzultace

konzultace s dozorovým úřadem, pokud z posouzení dopadů vyplývá vysoké riziko

upozornění na nedostatky, lhůta k odstranění

Spec.: konzultace poskytovaná orgánům státu při přípravě legislativních opatření

# A dále…?

revize unijní směrnice o soukromí v elektronických komunikacích

- přesnější pravidla pro služby informační společnosti
- zvláštní pravidla pro cookies
- on-line reklama

vodítka pracovní skupiny podle čl. 29 (WP29)
stanoviska Evropského sboru ochrany osobních údajů
nárůst case-law

novely zvláštních předpisů?

# Děkuji za pozornost.

Josef.Prokes@uoou.cz