Obecné nařízení o ochraně osobních údajů

předpis, který nahradí zákon o ochraně osobních údajů

úřad pro ochranu osobních údajů
the office for personal data protection

GDPR

účinnost v květnu 2018

náhrada směrnice 95/46/ES

regulace ochrany osobních údajů pro 21. století

reakce na nové technologie

revoluce i evoluce

GDPR ve zkratce

kontinuita se směrnicí 95/ES/46 / zákonem o ochraně osobních údajů

principy ochrany

základní pojmy - bez zásadních změn

práva subjektů údajů

povinnosti správců a zpracovatelů

nové nástroje ochrany údajů

celoevropský dozor

Staronové principy GDPR

zákonnost

férovost

přiměřenost / omezení účelem

minimalizace údajů

přesnost

odpovědnost

transparentnost

Nová konstrukce ochrany údajů

RBA / risk based assessment

privacy by design

privacy by default

accountability

Práva lidí dotčených zpracováním

být informován
mít přístup
uplatnit námitky

žádat

- opravu
- výmaz
- omezení
- přenesení údajů

Transparentnost a důvěra

vysvětlit zpracování

umožnit přístup k údajům / přenositelnost

varovat při narušení bezpečnosti

nadstandardně chránit citlivé údaje/rizikové agendy

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

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

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

uplatní se RBA - zohledňuje se stav techniky, náklady na provedení, kontext, účel

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

Pseudonymizace

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

záruka zpracování, snižuje rizika

„změkčuje“ povinnosti správců

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

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
soudní rozhodování - nárůst case-law

novely zvláštních předpisů?

Děkuji za pozornost.

Josef.Prokes@uoou.cz