

# VZTAH eIDAS K OCHRANĚ OSOBNÍCH ÚDAJŮ

aneb co bude znamenat nové nařízení GDPR pro  
elektronické transakce nejen ve veřejné správě

JUDr. Josef Donát, LL.M.

ROWAN LEGAL advokátní kancelář s.r.o.

# eIDAS a osobní údaje



## Preamble (11)

Toto nařízení by mělo být uplatňováno v plném souladu se zásadami ochrany osobních údajů podle směrnice Evropského parlamentu a Rady 95/46/ES. V tomto směru by se, s ohledem na zásadu vzájemného uznávání stanovenou v tomto nařízení, měla autentizace pro účely on-line služeb týkat zpracování pouze těch identifikačních údajů, které jsou přiměřené, podstatné a rozsahem úměrné pro udělení přístupu k dané on-line službě. Dále by poskytovatelé služeb vytvářejících důvěru a orgány dohledu měly dodržovat požadavky stanovené ve směrnici 95/46/ES týkající se důvěrné povahy a bezpečnosti zpracování.

- Viz dále i čl. 5 odst. 1

# eIDAS a osobní údaje



## Preamble (31)

Orgány dohledu by měly spolupracovat s orgány pro ochranu údajů, například je informovat o výsledcích auditů kvalifikovaných poskytovatelů služeb vytvářejících důvěru, jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů. Toto poskytování informací by se mělo týkat zejména bezpečnostních incidentů a narušení bezpečnosti osobních údajů.

- k tomu viz čl. 14 odst. 4 písm.f)

# eIDAS a osobní údaje



čl. 19

2. Kvalifikovaní a nekvalifikovaní poskytovatelé služeb vytvářejících důvěru vyrozumí orgán dohledu a případné další příslušné subjekty, jako jsou příslušný vnitrostátní orgán pro bezpečnost informací nebo orgán pro ochranu údajů, o každém narušení bezpečnosti nebo ztrátě integrity, jež mají významný dopad na poskytovanou službu vytvářející důvěru nebo na uchovávané osobní údaje, a to bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy toto narušení zjistili.

- k tomu též čl. 20 odst. 2

# Pozadí a dosavadní vývoj



- Dosud: Směrnice 95/46/ES + národní právní úprava (zákon č. 101/2000 Sb.)
- Nedávný vývoj
  - Rozhodnutí Google Spain: právo být zapomenut
  - Rozhodnutí Schrems: zrušení systému Safe Harbor
  - Nový systém Privacy Shield

# Pozadí a dosavadní vývoj



- Nově: Nařízení EP a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů)
- (2016/679)
  - Nařízení vs směrnice - posun k unifikaci pravidel, přímá účinnost v celé EU
  - Unifikace se ale zcela nepovedla
  - Návrh 2012 - vyjednávání - přijato v dubnu 2016
  - Účinnost od května 2018

# Základní pojmy a působnost



- **SUBJEKT ÚDAJŮ** = identifikovaná fyzická osoba nebo fyzická osoba, kterou lze přímo či nepřímo identifikovat prostředky, o nichž lze důvodně předpokládat, že je správce nebo jakákoli jiná fyzická nebo právnická osoba použijí pro identifikaci dané osoby, zejména s odkazem na identifikační číslo, lokalizační údaje, elektronický identifikátor nebo s odkazem na jeden či více zvláštních prvků její fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity

# Základní pojmy a působnost



- **OSOBNÍ ÚDAJ** = veškeré informace o subjektu údajů;



# Základní pojmy a působnost



**ZPRACOVÁNÍ** = jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, strukturování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace

# Základní pojmy a působnost



- **SPRÁVCE** = fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel, podmínky a prostředky zpracování osobních údajů; jsou-li účel, podmínky a prostředky zpracování určeny právem Unie či členského státu, je možné určit správce nebo zvláštní kritéria pro jeho jmenování na základě práva Unie nebo členského státu;

# Základní pojmy a působnost



- **ZPRACOVATEL** = fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje jménem správce;

# Základní pojmy a působnost



- Celá řada nových pojmů, které souvisejí s novými právy (omezení zpracování), povinnostmi (pseudonymizace) nebo rozdělením kompetencí mezi členskými státy (hlavní provozovna, dotčený úřad atd.)
  - Pojmy osobní údaj a zpracování bez podstatných změn
  - Platí i pro veřejný sektor
  - Výjimky z působnosti
    - Zpracování při činnostech, které nespadají do působnosti práva EU (např. národní bezpečnost)
    - Zpracování při činnosti související s politikou kontrol na hranicích, azylu a přistěhovalectví
    - Fyzickou osobou pro osobní a domácí potřebu
- Příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání TČ nebo výkonu trestů, vč. ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení

# Změny v právních důvodech zpracování



## ■ Souhlas

- S GDPR obtížnější získat, nejprve je třeba hledat jiné tituly
- Pokud existuje jasná nerovnováha mezi správcem a subjektem údajů, tak souhlas nestačí

## ■ Další právní tituly:

- Plnění smlouvy
- Splnění právní povinnosti na základě zákonné povinnosti s oporou v právu členské země či Unie
- Ochrana životně důležitých zájmů SÚ
- Veřejný zájem, výkon veřejné moci
- **Oprávněný zájem**

# Změny v právních důvodech zpracování



Čl. 6 odst. 2 - Členské státy mohou zachovat nebo zavést konkrétnější ustanovení, aby přizpůsobily používání pravidel tohoto nařízení ohledně zpracování ke splnění odst. 1 písm. c) a e) tím, že přesněji určí konkrétní požadavky na zpracování a jiná opatření k zajištění zákonného a spravedlivého zpracování, a to i u jiných zvláštních situacích, při nichž dochází ke zpracování, jak stanoví kapitola IX.

- odst. 1 písm. c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- odst. 1 písm. e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

# Nová práva fyzických osob



- Právo vznést námitku a právo na výmaz a (právo „být zapomenut“)
- Právo na přenositelnost údajů („portabilita“)
- Povinnost správce napomáhat uplatňování
  - Online formuláře, telefonní linky, ...

# Nové povinnosti v oblasti bezpečnosti



- Záměrná ochrana osobních údajů
- Standardní ochrana osobních údajů
- Náležitá technická a organizační opatření
- Hlášení bezpečnostních incidentů:
  - Dozorovému úřadu
  - Subjektům osobních údajů



# Nové požadavky na smlouvy



- Dopad na dodavatele IT systémů s přístupem k údajům
- Due diligence před uzavřením
  - Dostatečné záruky zavedení vhodných technických a organizačních opatření
- Zpracování pouze dle pokynů správce
  - Výjimky dle práva EU a členských států
  - Informování o požadavcích zákona
- Bezpečnostní opatření
- Součinnost při zabezpečení, hlášení incidentů, atd.
- Informační povinnost
- Audity, včetně prohlídek na místě

# Posouzení vlivu na ochranu osobních údajů místo registrace



- Povinnost oznamování dozorovému úřadu zrušena
- Místo toho: Posouzení, zda způsob zpracování neohrožuje práva a svobody jednotlivce a předchozí konzultace s dozorovým úřadem
  - Ve vybraných případech

# Pověřenec pro ochranu údajů jako nová role



■ Pro orgány veřejné moci povinné

■ Kvalifikace a postavení

- Expertní znalost práva a praxe ochrany OÚ
- Zaměstnanec / služba
- Informovanost, nezávislost, mlčenlivost

■ Úkoly

- Poučuje o závazcích z právních předpisů o OÚ
- Dohlíží na dodržování
- Spolupracuje s dozorovým úřadem, kontaktní osoba pro subjekty osobních údajů

# Výrazné zpřísnění sankcí



- Nově až 20 mil. EUR
- Čl. 89 odst. 7: Členské státy mohou stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat **správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.**

# Další kroky



- Příprava a vyčlenění compliance projektu
- Revize a úprava vnitřních předpisů
- Revize souhlasů a smluv
- Nastavení nových procesů (incidenty, dokumentace)
- Zajištění personálních kapacit pro plnění organizačních požadavků

**JUDr. Josef Donát, LLM**

*donat@rowanlegal.com*

[cz.linkedin.com/in/josefdonat](https://cz.linkedin.com/in/josefdonat)

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



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