APLIKACE GDPR VE VYSOCE REGULOVANÉM PROSTŘEDÍ

František Nonnemann

BANKOVNÍ SEKTOR

Veřejný zájem na stabilitě finančního trhu, proticyklická politika, ochrana spotřebitele → regulace bankovního sektoru

Regulované produkty, procesy, vnitřní správa a řízení bank, informační povinnosti, omezený vstup na bankovní trh…

Banky již dnes fakticky plní řadu nových povinností dle GDPR (ověření zpracovatele, analýza rizik, bezpečnost)

Odlišné regulace dopadající na stejné subjekty – racionální zákonodárce?

Nutnost pragmatického výkladu a respektování účelu předpisu

PRÁVA DOTČENÉ OSOBY

Současná práva:

- Právo na přístup k údajům (včetně kopie)
- Právo na opravu
- Právo na výmaz
- Právo na omezení zpracování

Nová práva:

- Právo na přenositelnost údajů
- Právo vznést námitku proti automatizovanému zpracování

PŘENOSITELNOST – ČL. 20

1. Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:

    a) zpracování je založeno na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) nebo na smlouvě podle čl. 6 odst. 1ísm. b); a

    b) zpracování se provádí automatizovaně.

…

4. Právem uvedeným v odstavci 1 nesmí být nepříznivě dotčena práva a svobody jiných osob.

PŘENOSITELNOST – REC. 68

Aby měl subjekt údajů větší kontrolu nad svými údaji, měl by v případě, kdy se osobní údaje zpracovávají automatizovaně, mít též právo získat osobní údaje, které se ho týkají, a jež poskytl správci, ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu a předat je jinému správci. Správce údajů je třeba podporovat v rozvíjení interoperabilních formátů umožňujících přenositelnost údajů. Toto právo by se mělo uplatnit v případě, kdy subjekt údajů poskytl osobní údaje na základě svého souhlasu, nebo pokud je zpracování potřebné za účelem plnění smlouvy… Pokud je to technicky možné, měl by mít subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci jinému.

VODÍTKO WP29 – PROBLEMATICKÉ BODY

Rozsah údajů: data odvozená z aktivity dotčené osoby (vč. transakčních údajů z bankovního účtu), hrubá data z chytrého měření či jiných připojených zařízení, záznamy o činnosti uživatele (logy)

Nové postupy: poskytnout přehled dat, ze kterých si dotčená osoba vybere, co chce poskytnout či přenést

Vztah k sektorové legislativě: posuzovat žádost spíše podle označení, nejasně vyjádřen vztah *lex specialis* a *legi generali*

PŘÍKLAD SEKTOROVÉ ÚPRAVY

Změna platebního účtu dle § 124j – §124p zákona o platebním styku
(§ 204 – 209 návrhu nového zákona o platebním styku):

- Povinnost provést změnu účtu
- Detailní náležitosti (rozsah údajů, povinnosti nové banky, informace pro plátce a příjemce o změně účtu)
- Možnost požadovat úhradu nákladů

PRÁVO NA PŘENOSITELNOST A SEKTOROVÁ ÚPRAVA

Účelem je mobilita služby stejně jako u přenositelnosti

Zvláštní úprava upřesňuje rozsah údajů, podmínky, úhradu

Obcházení zákona, zneužívání práva?

Nový správce nemá povinnost data přijmout

DATA BREACH

Nový princip odpovědnosti (accountability) přináší řadu nových administrativních povinností

Povinnost oznamovat ÚOOÚ případy porušení zabezpečení osobních údajů představující relevantní riziko pro dotčené osoby

Rozsah sdělovaných údajů, lhůty, formulář

Jedna událost může být incidentem podle více předpisů - GDPR, PSDII, NIS – s odlišnými pravidly pro notifikaci (lhůty, rozsah, způsob)

Efektivita, zátěž?

REPORTOVACÍ POVINNOSTI

Odlišné reportovací povinnosti obdobných či stejných incidentů

Příležitost pro stát nebo akademickou sféru najít řešení pro usnadnění a zefektivnění postupu dotčených subjektů i regulátorů

Společné rozhraní pro notifikování obdobných incidentů (GDPR, NIS, PSDII, ElKom), společný rozsah dat, logika předávání informací regulátorům

ZÁVĚR

Komplexitě a nepřehlednosti právního řádu lze čelit různě, jedním z nástrojů je racionální výklad práva

nonnemann@volny.cz