Dopad GDPR na zákaznické databáze obchodníků

Seminář Vybavení prodejny aneb – investice, které vám zvýší obrat, Praha 8.11.2017

Mgr. Bc. Milan Fric, LL.M.
Advokát
PricewaterhouseCoopers Legal s.r.o., advokátní kancelář

pwc

PwC Legal

GDPR: Obecné nařízení o ochraně osobních údajů

Nové nařízení o ochraně osobních údajů vstoupí v účinnost 25. května 2018 a **nahradí původní směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob** v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů z roku 1995.

Správce a zpracovatel osobních údajů

Správce osobních údajů

Správcem osobních údajů je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, **který sám nebo společně s jinými určuje účely a prostředky** zpracování osobních údajů.

Zpracovatel osobních údajů

Zpracovatelem osobních údajů je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje **pro správce.**

Zpracovávání osobních údajů

Co je osobní údaj?

Pokuty za porušení povinností stanovené nařízením

Vyšší pokuty

- GDPR výrazně navyšuje pokuty ukládané za porušování pravidel ochrany osobních údajů.
- Při vyměřování pokut je **posuzována závažnost porušení, délka trvání, povaha, rozsah a účel zpracování, míra škody** a další okolnosti.
- Vzhledem k výši pokut je doporučena vyšší míra orientace v oblasti ochrany osobních údajů také od vrcholného managementu.

max. 2 % – 4 % z obratu podniku; 10 – 20 milionů EUR

Zákonnost – právní důvod zpracování

Souhlas se zpracováním osobních údajů

Požadavky na souhlas

- **Informovaný, jednoznačný a svobodný**.
- Musí být stejně jednoduše odvolatelný, jako bylo jeho udělení.
- Při zpracování zvláštních kategorií osobních údajů musí být uveden výslovně.
- Správce musí být po celou dobu zpracování schopen tento souhlas doložit.
- **Podmíněný souhlas, který není nutný pro plnění dané smlouvy, je neplatný.**
- Splnění minimálního standardu informační povinnosti vůči subjektu údajů.

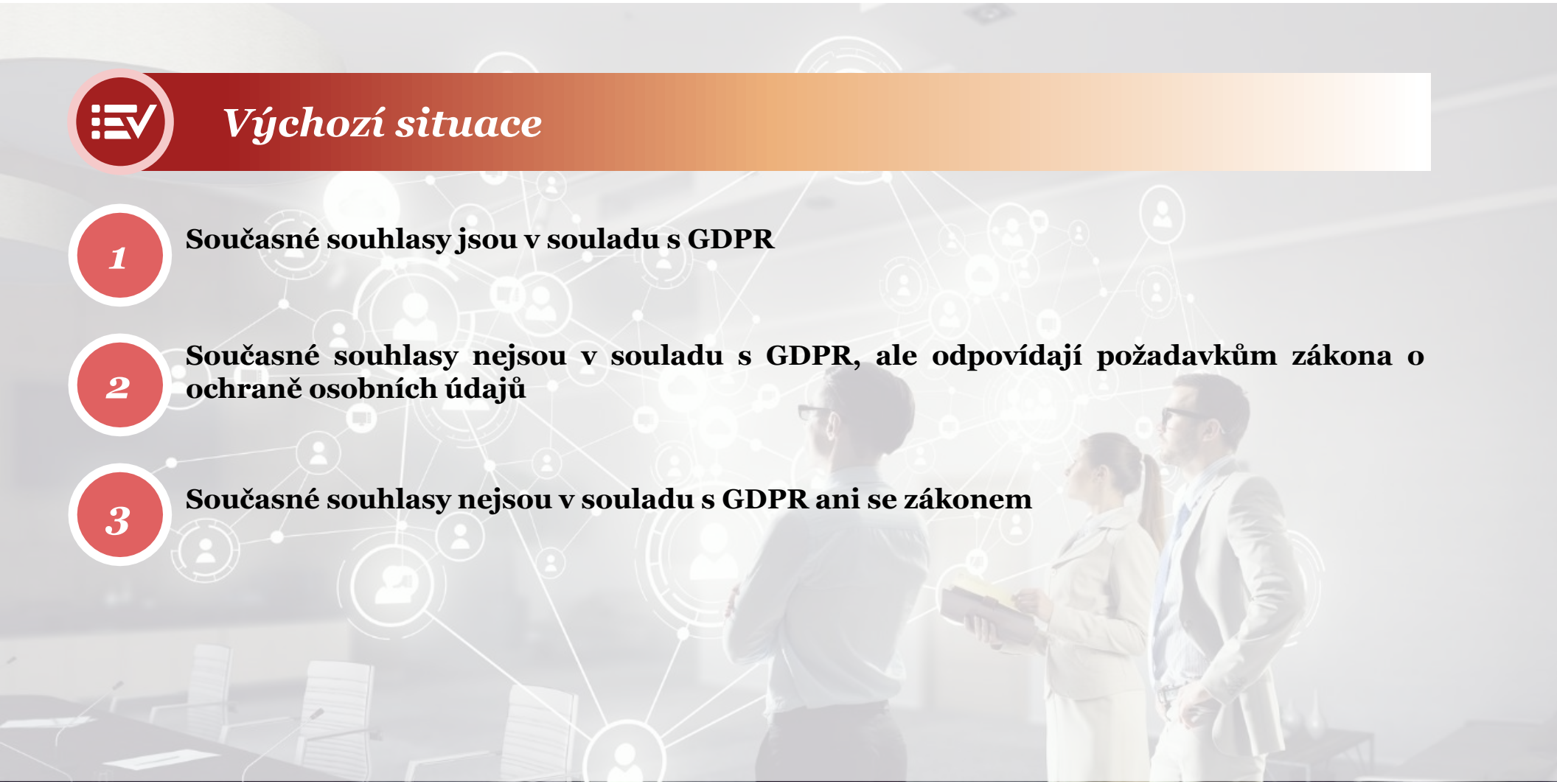
Souhlas dítěte pro služby informační společnosti

- Dle návrhu implementačního zákona v ČR musí být souhlas dítěte mladšího 13 let vyjádřen či schválen jeho zákonným zástupcem. Správce zároveň musí v rámci svých možností ověřit, že je daná osoba opravdu zákonným zástupcem dítěte.

Klientské databáze ve vztahu k GDPR

Výchozí situace

1. **Současné souhlasy jsou v souladu s GDPR**
2. **Současné souhlasy nejsou v souladu s GDPR, ale odpovídají požadavkům zákona o ochraně osobních údajů**
3. **Současné souhlasy nejsou v souladu s GDPR ani se zákonem**



1. Souhlas je v souladu s GDPR

1

- **Zpracování osobních údajů může pokračovat i nadále – recitál 171.**

*„Nařízení v recitálu 171 předpokládá **přechod souhlasu**, avšak **s podmínkou, že souhlas byl udělen způsobem a v souladu s podmínkami nařízení**. To bude pro mnoho správců problematické, jelikož jimi získávaný souhlas nebude splňovat podmínky stanovené v článku 7 Obecného nařízení, například podmínku **odlišitelnosti souhlasu** (souhlas nesmí být neoddělitelnou součástí obchodních podmínek) či podmínku **nepodmiňovat poskytnutí služby vyžadováním udělení souhlasu** se zpracováním osobních údajů.“* (zdůraznění přidáno)

Zdroj: Úřad pro ochranu osobních údajů, přístupné online: https://www.uoou.cz/4-zasady-a-pravni-duvody-zpracovani/d-27271/p1=0 (8.11.2017)

2

- **Bez dopadů na klientské databáze.**

3

- **Minimum případů.**

2. Souhlas je v souladu se současným zákonem

1

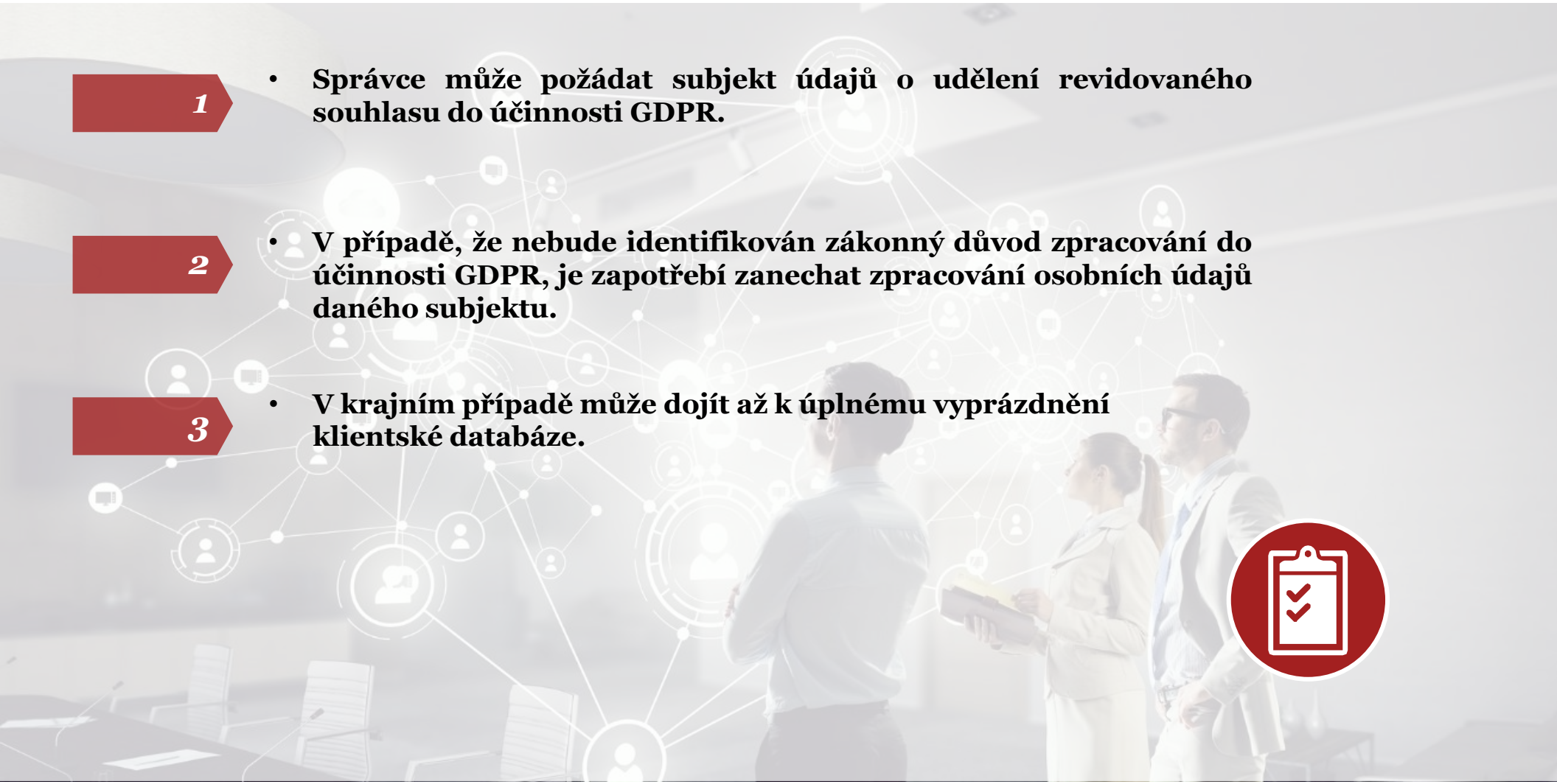
- **Správce může požádat subjekt údajů o udělení revidovaného souhlasu do účinnosti GDPR.**

2

- **V případě, že nebude identifikován zákonný důvod zpracování do účinnosti GDPR, je zapotřebí zanechat zpracování osobních údajů daného subjektu.**

3

- **V krajním případě může dojít až k úplnému vyprázdnění klientské databáze.**



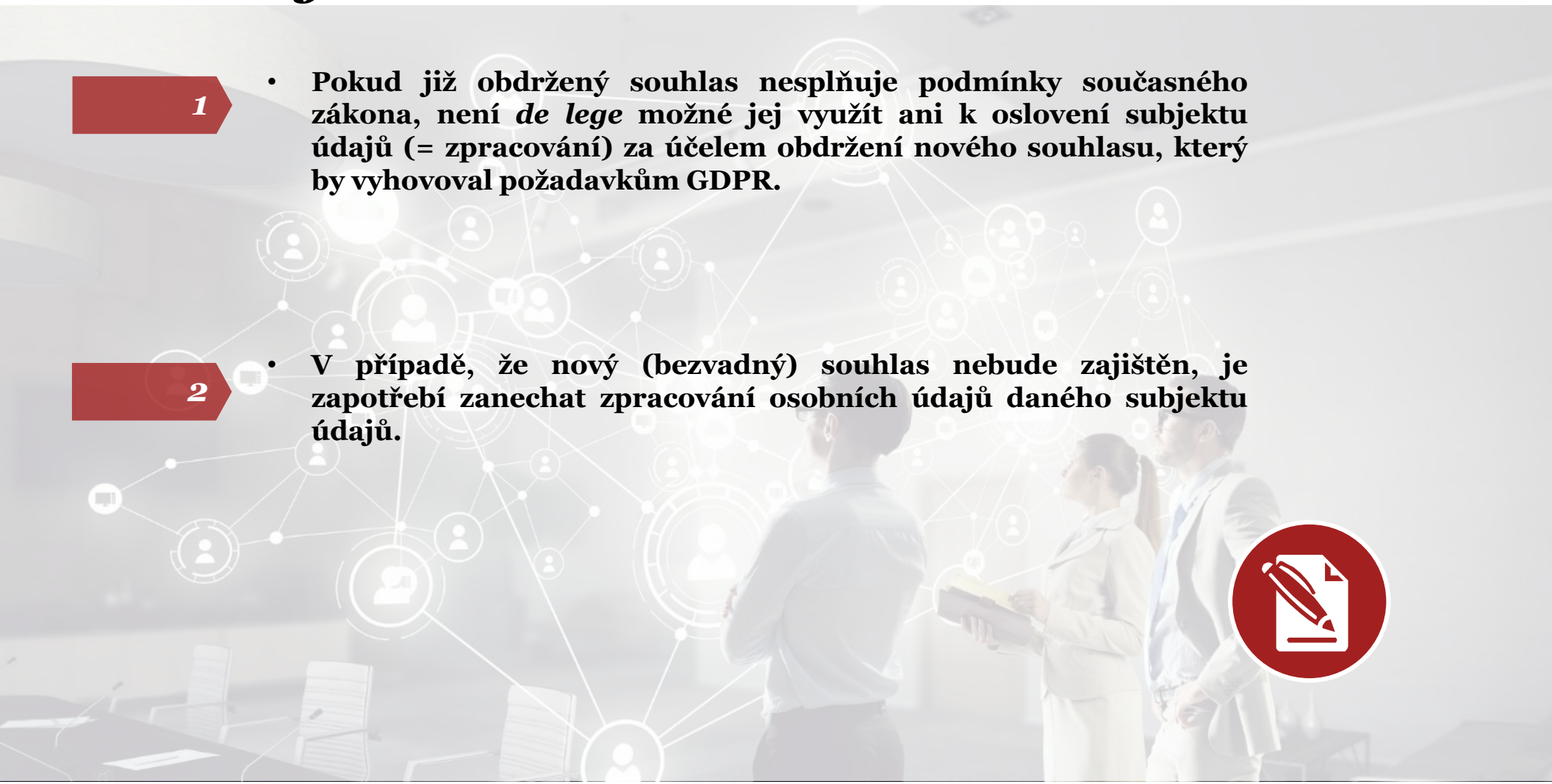
3. Souhlas není v souladu s GDPR ani se současným zákonem

1

- **Pokud již obdržený souhlas nesplňuje podmínky současného zákona, není *de lege* možné jej využít ani k oslovení subjektu údajů (= zpracování) za účelem obdržení nového souhlasu, který by vyhovoval požadavkům GDPR.**

2

- **V případě, že nový (bezvadný) souhlas nebude zajištěn, je zapotřebí zanechat zpracování osobních údajů daného subjektu údajů.**



Šíření obchodních sdělení na základě zákona o některých službách informační společnosti

1

- **Podrobnosti elektronického kontaktu subjektu údajů pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů, může správce využít pro potřeby šíření obchodních sdělení týkajících se jeho vlastních obdobných výrobků nebo služeb.**

2

- **Je pravděpodobné, že tuto formu přímého marketingu bude obecně možné považovat za oprávněný zájem správce ve smyslu recitálu č. 47 GDPR.**

  Z recitálu 47 Nařízení: *„Oprávněné zájmy správce, (…) se mohou stát právním základem zpracování za předpokladu, že* ***nepřevažují zájmy nebo práva a svobody subjektu údajů****, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem. Tento oprávněný zájem by mohl být dán například v situaci, kdy* ***existuje relevantní a odpovídající vztah mezi subjektem údajů a správcem****, například pokud je subjekt údajů zákazníkem správce nebo mu naopak poskytuje služby. (…) Zpracování osobních údajů pro účely* ***přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu****.“*

Koupě klientských databází podle GDPR

Nařízení zpřísněnými podmínkami na udělení souhlasu ke zpracování významně postihne mimo jiné také tzv. data-brokering, jehož obchodní model je postaven na prodeji/nákupu databází osobních údajů subjektů údajů za účelem jejich marketingového oslovování.

1

- **Při koupi klientské databáze kupující vstupuje do role správce a odpovídá mj. za to, že souhlasy se zpracováním jsou uděleny podle všech požadavků GDPR.**

2

- **Osobní údaje obsažené v zakoupených klientských databázích od třetích stran nebude možné zpracovávat bez identifikace legitimního důvodu zpracování.**

3

- **K prodeji databáze osobních údajů bude standardně vyžadován souhlas subjektu údajů, který se vztahuje na tento způsob předávání a následné zpracování.**

příklad

- **Vanquis Bank v září 2017 pokutována £ 75,000 britským regulátorem za zasílaní nevyžádaných obchodních sdělení na základě zakoupené databáze s nedostatečně určitými souhlasy.**

Doporučení na závěr

- Nepodceňujte přípravu ani možný rozsah implementačních opatření. Pro začátek doporučujeme vyhotovení tzv. gap analýzy ze strany zkušených odborníků. Tato analýza vám odhalí možná rizika a umožní vám vytvořit si konkrétní představu o potřebné časové náročnosti k jejich odstranění.

- Identifikujte právní důvod pro zpracování osobních údajů ještě před účinností GDPR a v případě potřeby připravte vhodnou žádost, popř. incentivu, k udělení revidovaného souhlasu.

- Rozlišujte mezi souhlasem se zpracováním osobních údajů k marketingovým účelům a zasíláním obchodních sdělení na základě zákona o některých službách informační společnosti.

Kontakt

Milan Fric

Advokát

Hvězdova 1734/2c
140 00 Praha 4
Česká republika
Mobil: +420 703 186 917
Email: milan.f@pwc.com

pwc

PwC Legal

Děkujeme za pozornost.

Informace obsažené v této prezentaci mají obecný charakter a neslouží jako zdroj odborného poradenství. Nedoporučujeme, abyste na základě těchto informací podnikali konkrétní kroky bez dodatečné odborné konzultace. Neposkytujeme žádná prohlášení ani záruky (výslovné ani učiněné mlčky), pokud jde o úplnost a přesnost informací obsažených v této prezentaci. PricewaterhouseCoopers Legal s.r.o., advokátní kancelář, její členové, zaměstnanci a spolupracovníci, v rozsahu povoleném příslušnými právními předpisy, neodpovídají za jakékoliv následky způsobené případným jednáním, zdržením se jednání, spoléháním se na informace obsažené v této prezentaci či jakýmkoliv rozhodnutím učiněným na základě informací v této prezentaci.

Tato prezentace je vytvořena na základě výkladových stanovisek Úřadu pro ochranu osobních údajů, WP29 a odborné veřejnosti ke dni vydání této prezentace. Doporučení uvedená v této prezentaci mají zvýšit soulad s GDPR. Nezaručují však soulad s GDPR ve 100% výši vzhledem k tomu, že při zpracování a vydání této prezentace stále probíhá proces přípravy výkladových pravidel a stanovisek Úřadu pro ochranu osobních údajů, WP29 a jiných českých a evropských institucí týkající se tohoto nového nařízení. Vzhledem k tomu, že v současné době je připravován návrh nového adaptačního zákona, který bude měnit český zákon o ochraně osobních údajů a související předpisy s cílem přizpůsobit české právo tomuto nařízení a stále neexistuje evropská či česká judikatura týkající se interpretace a správné aplikace tohoto nařízení, je nutné chápat doporučení v této prezentaci toliko jako doporučující, zvyšující soulad s teoretickým výkladem GDPR ke dni vytvoření této prezentace.