

GDPR a marketing

Marie Šebelová, advokátka

Praha, 10. ledna 2018

Témata příspěvku

- Hlavní změny, které GDPR přináší
- Pojmy
- Zásady GDPR
- Právní tituly zpracování OÚ podle GDPR
- Právní tituly zpracování pro marketing
 - Souhlas
 - Plnění smlouvy
 - Oprávněný zájem
- Praktické tipy pro dodržování GDPR

GDPR, právní rámec

- Nařízení (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (obecné nařízení o ochraně osobních údajů)
- GDPR = General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
- Nařízení je platné od 24.5.2017
- Od 25. května 2018 je použitelné (účinné) – bez dalšího je závazné a použitelné

GDPR, právní rámec

- Zákon č. 101/2000 Sb., o ochraně osobních údajů bude nahrazen zákonem o zpracování osobních údajů – návrh od MVČR je na vládě ČR
- Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním OÚ a o volném pohybu těchto údajů bude 25. května 2018 zrušena
- Pracovní skupina WP29 – vydává stanoviska a doporučení, vykládá GDPR
 - Pokyn k pověřenci
 - Pokyn k právu na přenositelnost
 - Pokyn k posouzení vlivu na ochranu OÚ
 - Pokyn k souhlasu
- Z pracovní skupiny WP29 vznikne k 25.5.2018 Evropský sbor pro ochranu OÚ

GDPR, právní rámec

- Zákon o zpracování osobních údajů – návrh od MVČR je na vládě ČR
- Co přinese:
 - Slučitelnost účelů
 - Věk dítěte pro souhlas se zpracováním OÚ – 13 let
 - Kdo je veřejný subjekt
 - ÚOOÚ – definování činnosti ve vztahu k GDPR
 -

GDPR, právní rámec

- Struktura GDPR
 - Preambule a vlastní normativní text
 - Preambule, tzv. recitály je jakási výkladová část. Bez informací z preambule bychom GDPR nerozuměli
 - Vlastní normativní text GDPR – zákonný text, práva a povinností atd.

GDPR – hlavní změny

- GDPR není revoluce
- GDPR přináší detailnější právní úpravu
- GDPR rozpracovává práva subjektů údajů a přidává nová práva (právo na přenositelnost)
- GDPR přináší nové povinnosti (ohlašování případů porušení zabezpečení OÚ, jmenování pověřence, vedení záznamů o zpracování OÚ)
- GDPR zavádí lhůty k plnění právních povinností (3 dny, měsíc)
- GDPR již nezná registraci u Úřadu pro ochranu osobních údajů
- GDPR zavádí vysoké pokuty v případě porušení

Pojmy

Zpracování osobních údajů

- jakákoliv operace s osobními údaji, např. shromáždění, zaznamenání, uspořádání, strukturování, uložení, pozměnění, vyhledávání, nahlédnutí, použití, šíření, seřazení, výmaz, zničení

Osobní údaj

- jakákoliv informace, která se týká identifikované nebo identifikovatelné osoby, např. jméno, datum narození, bydliště, telefon, e-mail, IP adresa, uživatelské jméno, lokační údaje, síťový identifikátor

Pojmy

Zvláštní kategorie osobních údajů (dříve citlivé)

- rasový či etnický původ, politické názory, náboženské či filosofické přesvědčení, členství v odborech, geometrické či biometrické údaje, zdravotní stav, sexuální orientace např. fotografie obličeje, rentgenový snímek, otisk prstu

Subjekt údajů

- fyzická osoba, které se údaje týkají

Pojmy

Správce

- Osoba, která určuje účel a prostředky zpracování

Zpracovatel

- Osoba, která zpracovává osobní údaje pro správce na základě jeho pokynů, zpracování se řídí smlouvou (povinné náležitosti čl. 28 GDPR)

Správce může být zároveň i zpracovatelem.

Zásady zpracování OÚ dle GDPR

- Zásada zákonnosti
- Zásada korektnosti a transparentnosti zpracování
- Zásada omezení účelu
- Zásada minimalizace zpracování OÚ
- Zásada přesnosti osobních údajů
- Zásada omezeného uložení OÚ
- Zásada integrity a důvěrnosti zpracování
- Zásada odpovědnosti

I. Zásada zákonnosti

- Každé zpracování musí mít právní základ = právní titul zpracování
- Právní tituly dle GDPR
 - Souhlas
 - Splnění smlouvy
 - Splnění právní povinnosti
 - Ochrana životně důležitých zájmů
 - Veřejný zájem nebo výkon veřejné moci
 - Oprávněný zájem

Právní tituly

- Plnění právní povinnosti
 - povinnost vyplývající z právních předpisů např.dle zákoníku práce, zákona o účetnictví, zákona o soc.či zdrav.pojištění
 - nerozšiřovat si povinnosti nad rámec zákonů, zpracovávat jen minimum dle zákonů
 - personálně-mzdová agenda x souhlas – užití OÚ nad rámec standardu, např. fotografie, zasílání informací o zaměstnancích mateřské společnosti

Právní tituly

- Ochrana životně důležitých zájmů
 - za účelem předejití vzniku újmy na životě subjektu údajů nebo jiné fyzické osoby, např. ošetření vážně zraněného, monitorování epidemií
- Veřejný zájem nebo výkon veřejné moci
 - zpracování OÚ orgány veřejné moci, pokud mají tuto povinnost za zákona

Splnění smlouvy

- Velmi častý právní titul
- V případě smluvního vztahu správce a subjektu údajů, např. koupě zboží, poskytnutí služby
- Zaniká s ukončením smlouvy, resp. reklamační dobou....

Právní titul - souhlas

- Svobodný, korektní, informovaný a jednoznačný projev vůle. Subjekt údajů souhlas poskytuje prohlášením nebo jiným zjevným potvrzením (tzv. aktivní souhlas)
 1. Svobodný a korektní souhlas – uzavření smlouvy nesmí být podmíněno udělením souhlasu atd.
 2. Jednoznačný – jasný pozitivní postup – zaškrtnutí políčka
 3. Informovaný – SÚ musí být před udělením souhlasu informovaný o všech skutečnostech zpracování dle čl. 12
- Odlišitelnost souhlasu – souhlas musí být oddělený od smlouvy či VOP
- Odvolatelnost souhlasu – subjekt údajů může souhlas kdykoliv odvolat, a to stejně snadně, jako ho udělil

Právní titul - souhlas

- Legální souhlasy
 - Obsahově bezvadné
 - Oddělené od ostatního obsahu
 - Aktivně udělené – zaškrtnutí, poskytnutí mailu x pokračování se službě
- Správce musí kdykoliv prokázat, že souhlas má
- Souhlas lze kdykoliv odvolat – stejně snadno, jako byl udělený

Přechod souhlasu

- předpoklad přechodu souhlasu – recitál 171 GDPR
- souhlas byl udělen způsobem a v souladu s GDPR
- souhlas nebyl udělen způsobem a v souladu s GDPR – dodatečné shojení nebo likvidace
- GDPR neumožňuje využívat OÚ, získané pasivním souhlasem, podmíněným souhlasem, souhlasem v rámci VOP nebo nákupem databází x DLE GDPR POUZE AKTIVNÍ SOUHLAS

Oprávněný zájem

- jeden z nejflexibilnějších právních důvodů – speciál 47 GDPR
- pro využití tohoto právního titulu by měl existovat relevantní a odpovídající vztah mezi subjektem údajů a správcem, např. zákazník správce x nikoliv vztah nadřazenosti – orgány veřejné moci
- zda subjekt údajů může zpracování OÚ důvodně očekávat
- před zpracováním OÚ na základě tohoto důvodu je třeba provést balanční test = zvážit, zda nad zájmem správce nepřeváží zájmy subjektu údajů
- např. zpracování osobních údajů pro účely přímého marketingu, ochrana majetku (kamery)

II. Zásada korektnosti a transparentnosti zpracování

- Správce má povinnost informovat subjekt údajů o zpracování OÚ
 - Informace o zpracování – čl. 13,14
 - Právo na přístup, opravu, výmaz, omezení zpracování, přenositelnost údajů a právo na námitku – čl. 15 – 22 – viz práva subjektu údajů
 - Oznámování bezpečnostních incidentů – čl. 34

Informační povinnost

- Správce má povinnost v okamžiku získání osobních údajů subjekt údajů informovat o:
 - Totožnosti správce
 - Pověřenci
 - Účelu a době zpracování
 - Příjemcích OÚ
 - Úmyslu předávat OÚ do EU
 - Právech subjektu údajů
- Proveditelnost poskytnutí informační povinnosti
 - Eshop – zpracovává na základě právního titulu plnění smlouvy - informační povinnost – po poskytnutí OÚ a před odesláním objednávky je mu sděleno, že pro plnění smlouvy jsou zpracovávány jeho OÚ
 - Zaměstnanci – informační dokument, který podepíše při nástupu

Oznámení bezpečnostních incidentů

- Nová povinnost dle GDPR – čl. 33-34
- Správce ohlašuje JAKÉKOLIV porušení zabezpečení ÚOOÚ do 72 hodin
- Zpracovatel ohlásí bezodkladně správci
- Správce ohlašuje porušení ÚOOÚ I subjektu údajů, pokud je RIZIKO pro subjekt údajů VYSOKÉ

III. Zásada omezení účelu

- OÚ musí být shromažďovány pro určité, výslovně vyjádřené, legitimní účely
- Od účelu zpracování se následně odvíjí právní důvod zpracování OÚ a také povinnosti správce, např. likvidace OÚ
- OÚ lze zpracovávat pouze pro daný účel, ten musí být vždy výslovně vyjádřen (informační povinnost správce)
- OÚ zpracovávané pro různé účely musí být oddělené
- Další zpracování OÚ – test slučitelnosti účelů

IV. Zásada minimalizace zpracování OÚ

- Zpracování vždy jen nezbytného množství osobních údajů ve vztahu k účelu, resp. právnímu titulu zpracování
- Zpracování z titulu zaměstnaneckého vztahu – fotografie?
- Zpracování z titulu splnění smlouvy – věk, datum narození?

V. Zásada přesnosti osobních údajů

- OÚ musí být přesné a aktualizované
- Správce musí přijmout opatření, aby byly OÚ opravovány
- GDPR nevyžaduje nákladné aktivní aktualizování

VI. Zásada omezeného uložení, integrity a důvěrnosti osobních údajů

- Zpracování OÚ lze jen po omezenou dobu, do naplnění účelu zpracování. Následně je třeba likvidovat či anonymizovat OÚ. Výjimka pro archivaci, výzkum a statistiku
- Integrita a důvěrnost = řádné zabezpečení osobních údajů – čl. 32 Nařízení
 - Vhodná technická a organizační opatření z hlediska povahy a účelu zpracování

VII. Zásada odpovědnosti

- Správce je povinnen zajistit dodržování GDPR a musí to být schopen prokázat/doložit
- Povinnosti správce
 - Zavedení vhodných technických a organizačních opatření, aby zajistil a byl schopen doložit, že zpracovává v souladu s GDPR
 - Vedení záznamů o činnosti zpracování
 - Odpovědnost za zpracovatele, smluvní vztah se zpracovatelem
 - Ohlašování bezpečnostních infidentů
 - Provedení posouzení vlivu na ochranu OÚ a předchozí konzultace
 - Zabezpečení osobních údajů
 - Ohlašování bezpečnostních incidentů

Záznamy o činnostech zpracování

- Každý správce (zpracovatel) vede záznamy o činnostech zpracování – čl. 30 GDPR
- Obsah záznamů je podobný jako nynější registrace na ÚOOÚ
- Záznamy se vyhotovují písemně nebo elektornicky
- Na vyžádání se poskytnou ÚOOÚ
- Výjimka pro firmy s méně než 250 zaměstnanci, pokud se jedná o příležitostné zpracování

Posouzení vlivu na ochranu osobních údajů

- Zpracovává se v případě, že daný druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob
 - Rozsáhlé a systematické automatizované zpracování včetně profilování
 - Rozsáhlé zpracování zvláštní kategorie OÚ
 - Při rozsáhlém a systematickém monitorování veřejných prostor
- ÚOOÚ zveřejní seznam druhů zpracování, které podléhají povinně posouzení vlivu

Pověřenec pro ochranu osobních údajů

- Pověřenec – DPO
- DPO dohlíží na dodržování GDPR, poskytuje školení a poradenství, spolupracuje s ÚOOÚ, je kontaktním místem pro subjekty údajů
- DPO se jmenuje v případech:
 - Zpracování OÚ orgány veřejné moci, vyjma soudů
 - Hlavní činnost správce/zpracovatele zahrnuje rozsáhlé, systematické a pravidelné monitorování subjektů
 - Hlavní činnost správce/zpracovatele zahrnuje rozsáhlé zpracování zvláštní kategorie OÚ

Pověřenec pro ochranu osobních údajů

- Pověřenec
 - interní – zaměstnanec
 - externí – na základě smlouvy o poskytování služeb

- Postavení DPO
 - Profesní kvality
 - Nezávislost
 - Zákaz sankcí za výkon funkce
 - Podléhá přímo nejvyššímu vedení
 - Zapojení do všech záležitostí spojených s ochranou OÚ
 - Povinnost mlčenlivosti
 - Zákaz střetu zájmů

Práva subjektu údajů

- Čl. 12-23 GDPR
- došlo k rozšíření stávajícího katalogu práv SÚ – k tomu paralelní nové povinnosti správce
 - Právo na informace o zpracování
 - Právo na přístup SÚ k OÚ
 - Právo získat od správce OÚ potvrzení o zpracování OÚ
 - Právo získat kopie zpracovaných OÚ
 - Právo na opravu
 - Právo na výmaz (právo být zapomenut)
 - Právo na omezení zpracování
 - Právo na přenositelnost OÚ
 - Právo vznést námitku v případě, že zpracování provádí správce na základě svých oprávněných zájmů

Právo na přístup k OÚ

- Právo na přístup k OÚ – čl. 15
 - Právo na potvrzení, zda správce OÚ zpracovává – do 1 měsíce, odpověď musí být kvalifikovaná dle čl.15/1, lhůtu lze prodloužit max. o 2 měsíce
 - Právo získat kopie zpracovaných OÚ

Úřad pro ochranu osobních údajů, pokuty

- Bude existovat nadále – pravomoci vyšetřovací, nápravné, povolovací a poradní
- Koordinace postupů jednotlivých úřadů států EU – Evropský sbor pro ochranu osobních údajů

Pokuty

- Až do výše 10 mil. EURO nebo do 2% celosvětového ročního obratu x dle zákona o zpracování osobních údajů 10 MIO pro veřejné subjekty
- Možné jen postihy – upozornění, napomenutí, zákaz nakládání s OÚ

Právní tituly, využívané pro marketing

- Souhlas
- Plnění smlouvy
- Oprávněný zájem

!!! Nezapomenout na zákon č. 480/2010 Sb., o některých službách informační společnosti – ANTISPAMOVÝ ZÁKON

- UŽ NEEEXISTUJE MARKETINGOVÁ VÝJIMKA

Reklama elektronickými prostředky

Reklamu lze EP zasílat pokud mám:

- Předchozí souhlas od adresáta
- Kontakt od zákazníka v souvislosti s prodejem výrobku nebo služby

Připravuje se Nařízení ePrivacy – bude také přímo účinné

Zpracování zveřejněných OÚ, marketingová výjimka

- GDPR neobsahuje ekvivalent právního důvodu, vedeného v § 5 odst. 2 písm. d) Zákona – tzv. marketingová výjimka
- Podle GDPR nebude již možné BEZ PRÁVNÍHO TITULU zpracovávat osobní údaje z veřejných rejstříků X podle Zákona šlo
- Dle GDPR je třeba pro marketing najít jeden z právních titulů

Právní důvod - souhlas

Charakteristika souhlasu - svobodný, korektní, informovaný a jednoznačný projev vůle. Subjekt údajů souhlas poskytuje prohlášením nebo jiným zjevným potvrzením (tzv. aktivní souhlas)

1. Svobodný souhlasu – uzavření smlouvy nesmí být podmíněno udělením souhlasu
2. Jednoznačný – jasný pozitivní postup – zaškrtnutí políčka
3. Odlišitelnost souhlasu – souhlas musí být oddělený od smlouvy, VOP, pravidel soutěže

Souhlas – jednoznačný, zjevný

Try SuperOffice CRM for free

Your name: *

Company name: *

Your email: *

Your phone: *

[Start Free Trial](#)

By signing up to a free trial of SuperOffice CRM, you agree to our [Terms](#) and you have read our [privacy policy](#). You may receive email updates from SuperOffice and you can opt out at any time.

Try SuperOffice CRM for free

Your name: *

Company name: *

Your email: *

Your phone: *

By signing up to a free trial of SuperOffice CRM, you agree to our [Terms and privacy policy](#).

Yes, please keep me updated on SuperOffice news, events and offers.

[Start Free Trial](#)

[Terms & privacy policy](#)

Právní důvod – oprávněný zájem

- speciál 47 GDPR - přímo uvádí, že oprávněný zájem je zpracování osobních údajů pro účely přímého marketingu
- splnění podmínky relevantního zákaznického vztahu
- právo subjektu údajů vznést námitku – čl. 21/2 – poté již nesmí být OÚ zpracovávány!!!

Praktické tipy pro dodržování GDPR – jak se na GDPR připravit

- analýza aktuálního nakládání s OÚ
 - analýza stávajících databází OÚ, rozsahu OÚ
 - analýza účelů zpracování OÚ
 - analýza přístupu k databázím a zabezpečení OÚ
 - analýza vnitřních předpisů ohledně OÚ

Praktické tipy pro dodržování GDPR – jak se na GDPR připravit

- Pokud zpracováváte na základě souhlasů:
 - Analýza souhlasů – svobodný souhlas, odlišitelnost souhlasu, aktivní souhlas - prostřednictvím zaškrtnutí políčka
 - podle výsledku analýzy
 - likvidace OÚ – nelze souhlas zhojit
 - další zpracování OÚ – souhlas odpovídá GDPR
 - znovuoobnovení souhlasu e-mailingovou kampaní

Praktické tipy pro dodržování GDPR – jak se na GDPR připravit

- Příprava potřebných dokumentů
 - Vnitřní předpis o zpracování OÚ
 - Záznamy o činnostech zpracování
 - Reakce na žádosti subjektu údajů
 - Ohlašování bezpečnostních incidentů

- Zvážit
 - Pověření
 - Posouzení vlivu na ochranu osobních údajů
 - Předchozí konzultaci

Děkuji za pozornost!

© 2018, Marie Šebelová, advokátka
www.aksn.cz

Tuto konferenci pořádá
Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz