

GDPR v praxi e-shopů

Marie Šebelová, advokátka

AK
SM
& Co.

ADVOKÁTNÍ KANCELÁŘ
ŠEBELOVÁ MARIE

Praha, 30. ledna 2018

Obsah

- Vývoj právní úpravy ochrany OÚ
- GDPR
- Hlavní změny, které GDPR přináší
- Pojmy – osobní údaje, zpracování osobních údajů....
- Zásady GDPR
- Právní tituly zpracování OÚ podle GDPR
- Právní tituly zpracování pro e-shopy
- Práva subjektů údajů
- Práva a povinnosti správců a zpracovatelů
- Praktické tipy pro dodržování GDPR

Vývoj právní úpravy ochrany OÚ

- Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním OÚ a o volném pohybu těchto údajů
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, uvnitř byla inkorporována směrnice 95/46/ES
- Překotný vývoj počítačové techniky, rozvoj internetu a sociálních sítí....
- GDPR (Obecné nařízení o ochraně osobních údajů)

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 24.5.2016
- 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:
 - Věk dítěte pro souhlas se zpracováním OÚ – 13 let
 - Výčet veřejných subjektů
 - Akreditační autorita - Český institut pro akreditaci, o.p.s.
 - 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
- fyzická osoba podnikající (IČař), 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.

Pojmy

Anonymizace

- Údaje jsou definitivně odděleny od subjektu údajů, již nelze nikdy spárovat.
- Anonymní údaje nejsou osobními údaji.
- Anonymizace je dána na roveň likvidaci.

Pseudonymizace

- Pseudonymní osobní údaje nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací.
- Dodatečné informace jsou uchovávány odděleně.

Pojmy

Rodná čísla

- Osobní údaj, nikoliv zvláštní kategorie osobních údajů. Reálně se jedná o tzv. kvazicitlivý údaj. Podmínky pro využití RČ jsou v zákoně o evidenci obyvatel a rodných čísel. RČ může užívat jen FO, které bylo přiděleno nebo jiná osoba, avšak jen v případech v zákoně uvedených.....
 - ministerstva, soudy, atd.
 - stanoví-li tak zvláštní zákon (zaměstnavatelská agenda)
 - se souhlasem

Kopírování OP

- Kopírování OP x číslo OP
- Zákon o občanských průkazech, kopie dle zvl.zákona či se souhlasem
- oblast bankovníctví....dle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
- Kopírování OP přes šablonu

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
 - Plnění smlouvy
 - Plnění 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, životopis.....personální spis po ukončení pracovního poměru

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

Plnění smlouvy

- Velmi častý právní titul
- Existuje smluvní vztah mezi správcem a subjektem údajů, např. zákaznický vztah, smlouvy mezi developerskou společností a klienty.
- Zvážit rozsah osobních údajů
- Zaniká s ukončením smlouvy, resp. reklamační lhůtou

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 zpracovávání dle čl. 13-14
- 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

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 –
dodatečná náprava nebo likvidace
- GDPR neumožňuje využívat OÚ získané:
 - pasivním souhlasem
 - podmíněným souhlasem
 - souhlasem v rámci VOP

Oprávněný zájem

- jeden z nejflexibilnějších právních důvodů – speciálně 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 práva subjektu údajů
- Výsledek balančního testu je třeba zaznamenat do dokumentu
- 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:
 - Správci
 - Údajích, jaké budou zpracovávány
 - Účelu a době zpracování
 - Příjemcích OÚ – další správci, nikoliv zpracovatelé
 - Úmyslu předávat OÚ třetích zemí
 - Právech subjektu údajů
- Informace mají být poskytnuty srozumitelně, jednoduše (standardizované ikony), vrstvené informace
- 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 OÚ ÚOOÚ do 72 hodin
- Zpracovatel ohlásí bezodkladně správci
- Správce ohlašuje porušení OÚ i subjektu údajů, pokud je RIZIKO pro subjekt údajů VYSOKÉ, bez zbytečného odkladu
- Lhůta 1 měsíc + 2 měsíce lze prodloužit

III. Zásada omezení účelu

- OÚ musí být shromažďovány a zpracovávány pro určité, výslovně vyjádřené, legitimní účely
- Účelem zpracování může být např. zasílání nabídek našich produktů a služeb, hodnocení spokojenosti našich zákazníků, plnění smlouvy, ochrana majetku zaměstnavatele, vedení personálního spisu
- Účel musí být vždy výslovně vyjádřen (informační povinnost správce)
- OÚ zpracovávané pro různé účely musí být vedeny odděleně
- Další zpracování OÚ – test slučitelnosti účelů – **VŽDY INFORMAČNÍ POVINNOSTI**

Př. čl. 6 odst. 4 GDPR, zpracování za účelem plnění smlouvy a ochrany majetku

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?

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

Vhodná technická a organizační opatření, zabezpečení OÚ

- Správce má povinnost zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracovává OÚ v souladu s GDPR
 - Dodržováním schválených kodexů
 - Uděleným osvědčením
 - Svými vnitřními předpisy.....
- Zabezpečení osobních údajů
 - Posouzení rizik pro SÚ, posouzení stavu techniky a rozsahu a účelu zpracování TOMU ODPOVÍDAJÍCÍ ZABEZPEČENÍ
 - Např. Pseudonymizace, šifrování, omezení přístupů, přístupová hesla.....

VII. Zásada odpovědnosti

- Správce je povinnen zajistit dodržování GDPR a musí to být schopen prokázat/doložit
- Povinnosti správce
 - Zejména:
 - Zavedení vhodných technických a organizačních opatření
 - Vedení záznamů o činnosti zpracování
 - Smluvní zabezpečení vztahu správce - zpracovatel
 - Ohlašování bezpečnostních incidentů
 - Provedení posouzení vlivu na ochranu OÚ a předchozí konzultace

Smlouva o zpracování osobních údajů

- Smluvní vztah správce a zpracovatele je v GDPR upravený podrobněji
- Správce je odpovědný za zpracovatele. Má si vybírat jen takové, kteří poskytnou dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby zpracování bylo v souladu s GDPR (kvalita zpracovatele!!!)
- Obsah smlouvy čl. 28 odst. 3 – předmět, doba trvání zpracování, povaha a účel zpracování, typ OÚ, povinnosti a práva správce
- Smlouva – formy smlouvy
- Stávající smlouvy – nahradit novými, dodatky...
- Řetězení zpracovatelů – je stále možné, vždy se souhlasem správce a smluvním zakotvením

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 elektronicky
- 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 a předchozí konzultace

- 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, odpověď musí být kvalifikovaná dle čl.15/1
 - Právo na kopie zpracovaných OÚ – další kopie mohou být za poplatek
 - Ve lhůtě 1 měsíc, max. se dá prodloužit o další 2 měsíce

Úřad pro ochranu osobních údajů, pokuty

- Úřad pro ochranu osobních údajů - OOÚ 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 20 mil. EURO nebo do 4 % celosvětového ročního obratu x dle zákona o zpracování osobních údajů 10 MIO Kč pro veřejné subjekty
- Možné jen postihy – upozornění, napomenutí, zákaz nakládání s OÚ

OÚ v e-shopu

- Právní tituly zpracování osobních údajů v eshopu:
 - Plnění smlouvy
 - Oprávněný zájem – nabízení produktů a služeb
 - Souhlas

OÚ v e-shopu

- Plnění smlouvy
 - využití osobních údajů jen pro naplnění smlouvy, účel zpracování – prodej produktu apod.,
 - dostát informační povinnosti,
 - hlídat minimalizaci osobních údajů
- Oprávněný zájem = přímý marketing
 - výsledek balančního testu – ok
 - informační povinnost – ideálně hned na začátku

OÚ v e-shopu

- Souhlas - obsah
 - totožnost správce
 - účel nebo účely zpracování osobních údajů
 - údaje, jaké budou zpracovávány
 - existence práva odvolat souhlas
 - informace o použití osobních údajů čistě automatizovaně, včetně profilování
 - informace o předávání osobních údajů do třetích zemí
 - předání OÚ jiným příjemcům
 - informace o právech subjektů údajů

OÚ v e-shopu

- souhlas vzhledem k jeho získání
 - jednoznačným aktivním právním jednáním
 - srozumitelný, jasný, případně vrstvený
 - oddělený od ostatního textu – mimo VOP

Správce má povinnost existenci souhlasu kdykoliv doložit. V případě elektronického souhlasu CESTU získání.

OÚ v e-shopu

- Analýza stávajících souhlasů
 - souhlasy jsou v souladu s GDPR
 - souhlasy nejsou v souladu s GDPR
 - likvidace
 - oprava souhlasů tak, aby byly v souladu – direct mail
- Příprava e-shopu na GDPR
 - ideálně již nyní
 - VOP
 - souhlasy
 - informační povinnost

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
- pokud zpracováváte na základě souhlasů:
 - analýza souhlasů – svobodný souhlas, odlišitelnost souhlasu, aktivní souhlas - prostřednictvím zaškrtnutí políčka

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



ADVOKÁTNÍ KANCELÁŘ
ŠEBELOVÁ MARIE

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



Naše znalosti
pro Váš úspěch