

GDPR

Ochrana osobních údajů v praxi terapeuta



Ing. Marika Kocurová

O čem se dnes budeme bavit?

- Co je to tedy to GDPR?
- Jaké jsou nyní platné zákony?
- Co se mne týká a co musím udělat?
- Jak to mám udělat?



GDPR

Nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

- *Nahradí Zákon č. 101/2000 Sb, o ochraně osobních údajů – platný od roku 2000 a bude doplněn dalším zákonem ke konci roku 2018.*

Osobní údaj – Co je a není???

+ 420 739 639 134

Marika Kocurová



Marika ze společnosti ECC

Your Public IPv4 is: 94.230.150.13

cookies

Facebook, Twiter

m.kocurova@joalis.cz

letadloM@seznam.cz



Konkretizujme si! Co je osobní údaj?

- **Informace týkající se konkrétní osoby nebo přímo či nepřímo k ní přiřaditelné**
- **Obecné**
 - Jméno, pohlaví, datum narození, stav, občanství, IP adresa, fotografie, RTG snímek, lokační údaje, cookies...
 - Počet dětí, věk, bankovní účet – pokud toto postačí ke konkrétní identifikaci dané osoby (pokud nepostačí, nejedná se o osobní údaj)
- **Organizační**
 - Pracovní nebo osobní adresa, pracovní nebo osobní telefon a email, ověřovací identifikační údaje, veškerá identifikační čísla vydaná státem
 - Šifrované údaje – někdo zná klíč a lze tedy podle nich najít konkrétní osobu

Co osobní údaje nejsou...

- Údaje o právnických osobách
- Anonymizované údaje – neexistuje možnost na dohledání konkrétní osoby (rozdíl proti pseudonymizovaným údajům)
- Údaje zemřelých osob – pokud podle nich nelze identifikovat osoby živé
- Veškeré údaje, podle kterých nelze identifikovat daného člověka.

POZOR! ČÍM VÍCE ÚDAJŮ MÁTE, TÍM VĚTŠÍ JE ŠANCE, ŽE SE DOSTANOU DO KATEGORIE OSOBNÍCH ÚDAJŮ. TÍM VĚTŠÍM RIZIKŮM SE S JEJICH OCHRANOU VYSTAVUJETE!!!

Citlivé osobní údaje!!!

JE NUTNÝ VÝSLOVNÝ SOUHLAS KLIENTA + MIMOŘÁDNÁ OCHRANA

- Rasový či etnický původ
- Politické názory
- Náboženské nebo filozofické vyznání
- **Členství v odborech**
- **Zdravotní stav**
- Sexuální orientace
- Trestní delikty nebo pravomocné odsouzení

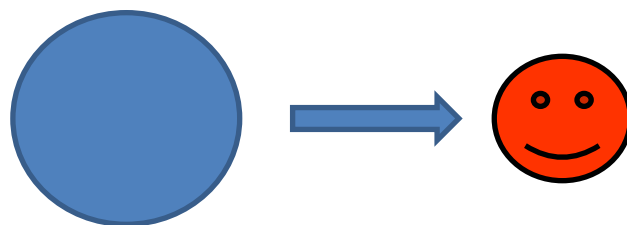
Řadí se sem i:

- Genetické údaje (DNA, krevní skupina)
- Biometrické údaje (otisk prstu, snímek duhovky)

DŮLEŽITÉ

POZOR! ČÍM VÍCE ÚDAJŮ MÁTE, TÍM VĚTŠÍ JE ŠANCE, ŽE SE DOSTANOU DO KATEGORIE OSOBNÍCH ÚDAJŮ. TÍM VĚTŠÍM RIZIKŮM SE S JEJICH OCHRANOU VYSTAVUJETE!!!

**SNAŽIT SE MAXIMÁLNĚ O
MINIMALIZACI DAT**



Takže:

Informace, které jsou přiřaditelné k člověku

+

Je to legálně proveditelné



Zpracování

=

**cokoliv, co se dělá s informací o
určité osobě.**

- Automatizovaně
- Částečně automatizovaně
- Ručně a je/půjde to do nějaké databáze/evidence

Zpracování

Základní zásady zpracování – povinnosti správce:

- Zákonnost
- Transparentnost
- Omezení účelem
- Minimalizace údajů a omezení uložení – musím vědět kam
- Přesnost
- Integrita a důvěryhodnost – zamezení zneužití
- Odpovědnost – zabezpečení a organizační opatření

Správce a zpracovatel

aneb (kdo je kdo)

Správce = „*Pán*“

- Ten, kdo určuje – co, kde, kdy, jak a proč
- Nese veškerou zodpovědnost za dodržování zákonnosti zpracování a to i za své zpracovatele

Zpracovatel = „*Sluha*“

- Zpracovává na základě pokynů Správce dané údaje – analyzuje, vyhodnocuje, mzdové účtárny atd...
- Nenese zodpovědnost
- Má však povinnost upozornit Správce na (ne)zákonné nakládání s údaji. Pokud tak neučiní je zodpovědný a stíhatelný i on.

Kdy zákon říká, že můžu (nebo musím)

GDPR:

- Plnění smlouvy (jednání o smlouvě)
- Oprávněný zájem
- Životní zájmy člověka
- Veřejný zájem
- Souhlas udělený danou osobou

Jiné zákonné důvody – povinnosti:

- Důchody, mzdy, odvody, zákoník práce

VŽDY MUSÍM MÍT ASPOŇ JEDEN PRÁVNÍ DŮVOD KE ZPRACOVÁNÍ OS. ÚDAJŮ. ALE SOUHLAS JE AŽ DRUHOTNÝM KROKEM.

Oprávněný zájem

Co je oprávněný zájem?

- Plnění smlouvy, servisu, služby...
- Moje marketingové aktivity potřebné k rozvoji firmy a obchodu...
- Přímý marketing a pod.
- Evidence docházky...

***Pokud sbírám údaje kvůli oprávněnému zájmu,
nepotřebuji souhlas.***

Oprávněný zájem však podléhá vyšším zájmům dané osoby – tj. její ochraně.

Jak na to?



VŽDY **INFORMUJTE** SVÉ KLINETY, PROČ
DANÉ ÚDAJE CHCETE!

Informační povinnost:

- Co...
- Kdo (správce, zpracovatel, pověřenec, další...)
- Účel - co budu s daty dělat?
- Zájem/povinnost – proč ta data chci?
- Doba – jak dlouho je budu mít v databázi?
- Dobrovolně/nutně – určení, zda musím nebo chci
- Práva – co vše může daná osoba vůči mně požadovat?

Souhlas

- Musí být jasně zřejmé, že jej klient potvrzuje – především problém webů
- Dál musí!!!
 - Být přiměřený
 - Být dobrovolný (pozor u zaměstnanců)
 - Být dvojité potvrzený – „Opt-in“ – u webu
 - Obsahovat popis práv
 - MUSÍ BÝT EVIDOVÁN!!!!
- Velký pozor na souhlasy od dětí!!!

Evidování souhlasu

- Kdo...
- Kdy...
- Jak souhlas zněl...
- Jak byl udělen (osobně, online...)
- Jestli byl odvolán a kdy...

Můžeme vést: písemně, elektronicky, pomocí logů/příznaky v online databázích

Pozor!!!

- NIKDY nesmíme jakoukoliv službu nebo třeba nákup zboží podmiňovat udělením souhlasu se zpracováním osobních údajů.
- Vždy musí být možné danou službu nebo zboží získat bez souhlasu.

(např. mohu na webu použít: „Pokud nám dáte souhlas se zpracováním osobních údajů získáte Abecedu detoxikace ZDARMA.“

Lze, protože zákazník má možnost si ji i zakoupit. Je proto důležité třeba zdůraznit informaci o ceně bonusu.

Tedy: „Získejte Abecedu detoxikace v hodnotě 55 Kč ZDARMA za udělení souhlasu.“)

Transparentnost

- Správce je povinen poskytovat transparentní informace o zpracování dat
- Řádně a včas zajistit uplatnění práv majitele osobních údajů.

Je potřeba nikdy nezatajovat ani nezkreslovat pravdu o zpracování, získávání a dalších informacích týkajících se osobních údajů. Tyto informace by měly být nějakým způsobem přístupné, aby se s nimi mohl zákazník/klient seznámit.

Musíme mít také vytvořen proces, který jasně definuje jakým způsobem přistupovat k případným žádostem majitelů osobních údajů. Tj. v případě, kdy jsem požádání o informace o tom, co, jak a proč zpracováváme, zda vůbec zpracováváme, případně jak je zajištěna skartace/výmaz údajů z naší databáze.

Omezení účelem

- Osobní údaje mohou být zpracovány pouze pro určité, výslovně vyjádřené a legitimní účely a nesmí být dále zpracovány způsobem, který s nimi není slučitelný.
- Výjimky pro zpracování i pro jiné účely:
 - Souhlas subjektu údajů
 - Povoleno nebo požadováno právním předpisem
 - Jedná se o slučitelný účel (test slučitelnosti) – balanční test (podobnost výrobků a služeb)

Jestliže tedy deklarujeme, že os. údaje zpracováváme čistě za účelem rozesílky informačních newsletterů, nesmíme je zpracovávat ještě za jinými nezveřejněnými účely, např. různé statistiky a výzkumy...

Minimalizace rozsahu a přesnost

- Uchovávat pouze relevantní údaje se vztahem ke službě
- Dané údaje jsou nezbytné pro daný účel

Dodržovat principy záměrné a standardní ochrany údajů

- Záměrná ochrana – vždy předem zvažovat ochranu
- Standardní ochrana – zpracovávat pouze nezbytné údaje

Přesnost

- Údaje musí odpovídat skutečnosti – jakákoliv změna se musí zapsat ihned – **aktualizace údajů**
- Následná likvidace a výmaz neplatných údajů

Minimalizace doby uchování

- Data uchovávat pouze po dobu nezbytně nutnou (nejčastěji 3 roky).
- Nutně musíte informovat o době zpracování.

Po této době musí být data vymazána a musí být jasně dokladováno: Jak a kdy byla data vymazána!!!

Odpovědnost

- Zavedení vhodných organizačních a technických opatření – doložení souhlasu
- Opatření následně aktualizovat
- Proaktivní opatření – ještě před udáním souhlasu
- **Povinná dokumentace**
 - Analýza rizik
 - Přijatá bezpečnostní opatření
 - Nastavení procesů (výkon práv majitelů údajů, oznámení incidentů)
 - Interní a externí dokumentace (souhlasy, oznámení, postupy, směrnice atd)

Práva majitelů údajů

- **Právo na přístup**
 - Potvrzení, zda jsou nebo nejsou osobní údaje zpracovány, účel zpracování, právní titul
 - Právo na kopii zpracovaných údajů
 - Právo na stížnost
- **Právo na opravu či doplnění os. údajů**
 - Bez zbytečného odkladu
- **Právo na omezení zpracování osobních údajů**

Zpracovatelské smlouvy

- Pokud pro nás zpracovává osobní údaje i někdo další
- Smlouva by Vám měla být nabídnuta, například v případě FB, google, správců webů a serverů.
- Pokud někdo zpracovává pro Vás, budete pravděpodobně muset vytvořit.
- Velký pozor na správné znění, abyste nepřevzali zodpovědnost za cizí pochybení

Směrnice

- Určují nám tok osobních údajů
- Určují nám účel zpracování
- Určují nám bezpečnostní procesy
- Určují nám vztahy

Vytvořit si nejlépe velmi jednoduché grafické znázornění či slovní vyjádření toku informací a dalších procesů.

Co tedy musím udělat?

Vytvořím si šanon/složku, která bude obsahovat tyto dokumenty:

Informace o správci dat

- Zde se představíte – kdo jste, IČO, sídlo..., co děláte (poradenství v oblasti životního stylu), jak to děláte, proč potřebujete osobní údaje (plnění služby a následný servis), co s těmito údaji děláte (evidence v databázi kvůli plnění služby a následného servisu) – vše jen opravdu velmi stručně.
- Musíte zde i uvést, kde mohou klienti uplatnit svá práva na informace – email a písemně na adrese
- Toto je veřejný dokument, který byste měli v případě žádosti poskytnout klientům a měli byste jej mít na svých provozovnách nebo místech provozování živnosti.

Co tedy musím udělat?

Sestavím si **analýzu rizik**, která bude obsahovat:

- **Zdroje dat** – odkud mi přichází osobní údaje – poradna, vlastní web, přednášky, emailová komunikace, telefon...
- **Jak data zpracovávám** – vkládání do databáze EAMset, zapisování návštěv do tištěné kartotéky, zálohování na disc/USBflash, předávání externí účetní, webové stránky, emailová komunikace...
 - Jako podbod, co konkrétně zpracovávám – jméno, datum narození....
- **Místa uložení dat** – EAMset, tištěná kartotéka, různé externí nosiče, cloud...
- **Možná bezpečnostní rizika** – vždy беру v potaz všechny předchozí možnosti, tj. počítač mi mohou zcizit, mohu jej ztratit, mohou mi vykrást poradnu, mohou mi napadnout mailový účet...

Co tedy musím udělat?

- **Měli byste si pro každé místo a proces určit míru rizika.**
- Používejte nejčastěji stupnici 1-5

Stupnice hodnocení:

1. Zanedbatelná nebo (žádná)
 2. Nízká
 3. Střední
 4. Vysoká
 5. Velmi vysoká
- Do tabulek od ECC si tedy číselně určíte míru bezpečnostního rizika na této stupnici. Dle výsledného čísla je poté potřeba určit potřebnou výši zabezpečení.

Co tedy musím udělat?

Určím si **Přijatá bezpečnostní opatření**

- Zde musím vždy ctít pravidlo – **míra rizika mi určuje výši zabezpečení** – u citlivých osobních údajů, vždy vyšší zabezpečení.
- **Pro každé místo uložení dat a případně i pro riziková místa předávání osobních údajů si určím zabezpečení...**
- Skříň – je zamčená v místnosti, je zamčená sama o sobě...
- PC, telefon, externí disc, USBflash – vždy pod mým dozorem nebo v uzamčeném prostoru... vše mám zabezpečeno heslem...
- Emailový účet – zabezpečen silným heslem – podívejte se na VOP poskytovatele, jaké uvádí zabezpečení...

Co tedy musím udělat?

Nastavit si proces **Výkonu práv subjektů údajů**:

- Určuje nám, jak budeme postupovat, když budou chtít klienti uplatnit svá práva na ověření, zda, co a v jakém rozsahu o nich zpracováváte...
- Určuje, kde Vás mohou klienti kontaktovat.
- Dávejte si rozumnou dobu na odpověď, nejlépe 14dní na odpověď, ale musíte ji poté dodržet. 24 hodni je nereálné a déle jak 14dní je již spíše neakceptovatelné...
- Musíte mít zpracovanou tabulku, kde budete vést: kdo, kdy, jakým způsobem a o co Vás požádal a kdy jste jeho žádost zpracovali.

Co tedy musím udělat?

Výkon práv subjektů údajů:

- Tabulky musím mít samostatně na – žádost o změnu, výpis z databáze a žádost o výmaz/skartaci...

Dále musíte mít vedenou tabulku – **Výmaz po uplynutí doby možné pro uchování dat** – to jsou ty tři roky od posledního plnění služby.

- Zde si budete vést záznamy o vymazaných osobních údajích o klientech, kteří u vás nebyli déle jak tři roky. Určete si rozumný interval, kdy budete kontrolovat své databáze – 3,6měsíců... šest měsíců je však maximální doba.

Co tedy musím udělat?

- Jako poslední věc si do šanonu přidám **souhlasy se zpracováním osobních údajů**, které jsou však až úplně poslední věcí, která je pro splnění GDPR potřeba...
- Ještě je potřeba si uvědomit, zda nepotřebuji **Zpracovatelské smlouvy** – které zastřešují to, když zpracováváte osobní údaje získané od jiného správce nebo naopak vy někomu údaje předáváte
- Nejčastěji to bývá: externí účetní, spolupráce v rámci poradenských center, webmasterské služby, ale i FB a další...

Děkuji za pozornost

Pokud budete mít nějaké dotazy, tak mne kontaktujte na „mých osobních údajích“



Ing. Marika Kocurová
Email: m.kocurova@joalis.cz