

Co znamená GDPR?

GDPR, neboli General Data Protection Regulation, známé také jako obecné nařízení o ochraně osobních údajů, je legislativa Evropské Unie, která výrazně zvyšuje ochranu osobních dat v členských státech EU.

GDPR bylo přijato všemi členskými státy EU již v dubnu 2016, účinnosti ale nabylo až dnem 25. 5. 2018.

GDPR představuje základní právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva jednotlivců proti neoprávněnému zacházení s jejich osobními údaji. Týká se tedy všech společností, institucí a subjektů, které s těmito daty nakládají a využívají je.

Porušení zásad GDPR je postihováno vysokými až astronomickými sankcemi

Jaké osobní údaje je nutné chránit v rámci GDPR?

GDPR ošetřuje ochranu veškerých osobních údajů všech fyzických osob. Tyto údaje se dělí do několika kategorií. Tyto údaje je možné zpracovávat pouze v rozsahu stanoveném v Obchodních podmínkách systému FKP.

KATEGORIE OÚ (osobních údajů)

1) Obecné osobní údaje – jméno, příjmení, adresa, trvalé bydliště, doručovací adresa, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, zdravotní znevýhodnění, fotografický záznam, video záznam, audio záznam, e-mailová adresa, telefonní číslo, IP adresa, různé identifikační údaje vydané státem (IČ, DIČ, číslo občanského průkazu, číslo řidičského pasu, číslo cestovního pasu atd.), dosažené vzdělání, příjmy ze zaměstnání, příjmy z důchodu, kulturní profil, osobní údaje manžela/manželky, dětí, partnera/partnerky aj.

2) Zvláštní kategorie osobních údajů – např. rasový či etnický původ, politický názor, náboženské vyznání, filozofické vyznání, členství v odborech, zdravotní stav – údaje o tělesném nebo duševním zdraví, o poskytnutí lékařské péče, sexuální orientace, trestní delikty, pravomocná odsouzení,

Genetické osobní údaje – např. DNA, RNA, krevní skupina, Rh faktor,

Biometrické osobní údaje – snímek obličeje, otisk prstu, snímek oční duhovky, snímek sítnice, podpis, zbarvení hlasu.

Společnost MEDICALELIX s.r.o. nezpracovává žádné osobní údaje patřící do zvláštní kategorie osobních údajů.

Základní principy GDPR:

- 1) Zákazník musí být informovaný o rozsahu a způsobu zpracování jeho OÚ.
- 2) Zákazník má právo vznést námitku ke zpracování jeho OÚ – na základě tohoto nebude správce OÚ moci tyto OÚ dále zpracovávat.
- 3) Správce OÚ má právo na přenositelnost OÚ na jiného správce, jestliže jsou údaje zpracovávány automatizovaně.
- 4) Zákazník musí mít online přístup k údajům, které jsou o něm shromažďovány.

5) Zákazník má právo na výmaz jeho OÚ a právo být zapomenut – díky tomu může zákazník požadovat okamžité smazání jeho OÚ, pokud neexistuje právní důvod pro jejich další zpracování.

6) Zákazník má právo podat stížnost na rozsah a způsob zpracování osobních údajů u dozorového orgánu, tj. u Úřadu pro ochranu osobních údajů.

Zahájení činnosti

Společnost RP Class s.r.o (později MEDICALELIX s.r.o.) – dále jen MEDICALELIX, od svých zákazníků a poradců bez výjimky vyžaduje důsledné dodržování všech principů ochrany osobních údajů. Zároveň MEDICALELIX je povinna zajistit, aby veškeré osobní údaje zákazníků a poradců byly chráněny v nejvyšším bezpečnostním režimu.

I poradce či zákazník MEDICALELIX musí svou práci uzpůsobit nařízení GDPR a veškeré jemu svěřené osobní údaje zákazníků společnosti MEDICALELIX musí chránit proti jakémukoliv úniku a zároveň se svými zákazníky jednat s naprostou diskrétností v přístupu k jeho osobním údajům.

Jak správně zajistit Vaše zařízení proti úniku dat?

Doporučujeme co nejlépe zajistit notebook, PC, mobilní telefon a veškerá další zařízení, která používáte ke komunikaci se zákazníky tak, aby se zamezilo jakémukoliv úniku dat.

V tomto bodu je nejdůležitější slovo HESLO. Nejjednodušší způsob primární ochrany dat je nastavit si na svém zařízení „neprůstřelné“ heslo, tj. heslo o minimálně osmi (8) znacích, které obsahuje velká a malá písmena, symboly a číslice a které budete pravidelně měnit. Samozřejmě při opuštění zařízení se nezapomínejte odhlašovat.

Samotné heslo ale pro eliminaci všech možných nebezpečí nestačí. Hackerské útoky (či různé výpadky) jsou v této době na denním pořádku a je nutné svá zařízení ochránit i prostřednictvím dalších nástrojů, aby se míra rizikovosti úniku dat snížila na minimum.

Desatero pro zajištění maximální bezpečnosti ochrany osobních údajů

1. Využijte široké nabídky antivirových programů.
2. Pravidelně aktualizujte virové databáze.
3. Mějte vždy nainstalovaný antivirový program, a to jak v počítači, tak i v jiných chytrých mobilních zařízeních.
4. Nezapomínejte také udržovat Váš operační systém (a obecně software) v aktuálním stavu - výrazně tím snižujete riziko možnosti napadení dat (např. u systému Microsoft Windows je to pomocí Windows Update). U mobilních telefonů a tabletů, či dalších „chytrých“ zařízení s operačními systémy Android nebo iOS je nutné pravidelně stahovat aktualizace (buď přímo v Google Play/App Store nebo v Nastavení zařízení).

5. Snažte se využívat zabezpečené a důvěryhodné internetové připojení, a naopak se vyhněte veřejným bezdrátovým přístupovým bodům.
6. Ve svém zařízení používejte pouze známý důvěryhodný software, bez instalace pochybných „programků“ a utilit.
7. Neotevírejte a v žádném případě nestahujte e-maily a jejich přílohy s neznámým obsahem či odesílatelem.
8. Nesdělujte své přístupové údaje žádným dalším osobám. Předáváte jim tak přístup nejen ke svým osobním údajům, ale i k údajům Vašich podřízených či Vašich zákazníků.
9. Pracujte s rozvahou a nestahujte vše, co reklamní bannery skrze internet nabízí.
10. Důvěryhodnost zabezpečení stránky zvyšuje šifrování https, které poznáte v adresním řádku (<https://www.medicalelix.cz/>). Případně se před ní zobrazí symbol zámku s textem zabezpečeno.

Praktické fungování GDPR v síti MEDICALELIX?

Každý dlouholetý poradce MEDICALELIX či zapálený nový poradce MEDICALELIX se sám sebe jistě ptá, jaké dopady má nařízení GDPR na fungování sítě MEDICALELIX poradců a zákazníků?

V kostce Vám popíšeme, co všechno znamená GDPR pro fungování sítě MLM, a s čím je nutné zákazníky před uzavřením registrace seznámit.

Základním principem fungování obchodu v rámci GDPR je okamžitá odvolatelnost souhlasu zákazníka se zpracováním osobních údajů k danému účelu.

Aby byly všechny souhlasy požadované v rámci sítě MEDICALELIX pro zákazníka a poradce dobře čitelné a správně pochopitelné, rozhodli jsme se rozdělit tyto souhlasy do několika kategorií.

Kategorie souhlasů za účelem naplnění povinnosti GDPR a jiných právních předpisů:

1) Souhlas s Obchodními podmínkami systému FKP MEDICALELIX

2) Souhlas se zasíláním marketingových a obchodních materiálů v elektronické formě – je obsahem OP MEDICALELIX

Souhlas s Obchodními podmínkami FKP MEDICALELIX

Zákazník registrací do systému FKP potvrzuje, že byl seznámen s principem fungování MLM sítě MEDICALELIX a že plně souhlasí se zpracováním jeho osobních údajů v rámci celé sítě MEDICALELIX – jeho osobní údaje využívají poradci, zákazníci a společnost MEDICALELIX pro obchodní a marketingovou komunikaci. Zároveň zákazník akceptuje zásady bezpečného zacházení s osobními údaji poradců a zákazníků, se kterými spolupracuje.

Udělení souhlasu je povinné pro každého zákazníka, který chce provést registraci do systému FKP nebo provést nákup zboží MEDICALELIX přes nákupní formulář FKP, či chce využívat dalších bonusů a výhod ze sítě MEDICALELIX viz. OP bod 4.4.8.

Souhlas je kdykoliv odvolatelný, v důsledku odvolání souhlasu se zruší celá zákaznickova registrace a nelze si na tuto zrušenou registraci již znovu objednat, nebo registraci obnovit. K vymazání OÚ dojde neprodleně po obdržení odvolání tohoto souhlasu, nejpozději však do sedmi (7) pracovních dní. MEDICALELIX zároveň informuje přímého nadřízeného poradce o vyřizování této žádosti od jeho zákazníka.

OÚ, které zákazník při udělení souhlasu musí uvést: Jméno, příjmení, fakturační adresa, doručovací adresa, země, mobilní telefon, e-mail.

V případě zahájení spolupráce s fyzickou osobou podnikající (tzv. „na živnostenský list“) je nutné doplnit tyto OÚ: IČO, DIČ, bankovní účet

Souhlas se zasíláním marketingových a obchodních materiálů v elektronické formě

Zákazník udělením souhlasu potvrzuje, že mu MEDICALELIX může zasílat marketingové a obchodní materiály v elektronické podobě moderními online i offline komunikačními kanály – eshop, directmailing, e-mailing, facebookový profil společnosti, online reklamní kampaně.

Souhlas je kdykoliv odvolatelný, v důsledku odvolání souhlasu zůstává registrace zákazníka platná a zákazník může i nadále objednávat zboží.

OÚ, které zákazník při udělení souhlasu musí uvést: E-mail a heslo.

Tyto údaje není nutné znovu vypisovat, dochází k jejich automatickému generování z údajů získaných ze souhlasu s Obchodními podmínkami MEDICALELIX.

Všechny osobní údaje uvedené v daných kategoriích souhlasů se zpracovávají v zabezpečených databázích na zašifrovaných serverech vlastněných MEDICALELIX. Není tedy nutné se obávat o jejich interní zneužití.

V případě nezajištění bezpečnosti při zpracovávání a zacházení s osobními údaji ze strany poradce MEDICALELIX či zákazníka MEDICALELIX, může MEDICALELIX tohoto poradce či zákazníka sankcionovat a při hrubém či opakovaném porušení s ním okamžitě ukončit spolupráci (tj. bez výpovědní doby).

Doporučení pro poradce MEDICALELIX při práci s osobními údaji

Jak pracovat s vlastními „speciálními“ záznamy o zákazníkovi?

Pokud si poradce MEDICALELIX vede podrobné záznamy o svých zákaznících, které mu pomáhají optimalizovat nabídku k objednávce, je nutné myslet na několik důležitých bodů:

1. Taková databáze, evidence, či přehled, není vlastnictvím MEDICALELIX – vlastník (správce) je poradce, který je za tuto databázi plně zodpovědný.

2. Databáze nemusí obsahovat pouze osobní údaje, ale i velmi citlivé údaje se zvláštním režimem, které je nutné chránit velmi pečlivě.
3. Poradce musí v tomto případě dbát na vysokou míru zabezpečení a s těmito údaji pracovat s nejvyšší opatrností a v souladu s právními předpisy.
4. Zákazník, kterého se tyto záznamy týkají, musí být dopředu informován, že dochází k jejich ukládání a musí poradci k tomu dát písemný souhlas.
5. V případě jakéhokoliv nesouhlasu se zpracováním OÚ ze strany zákazníka, je nutné okamžitě požadavku vyhovět a OÚ ze své databáze vymazat.

Práce s vlastními marketingovými komunikačními nástroji

Využíváte-li ke své práci osobní webová stránka poradce, facebookovou skupinu, stránku či profil, anebo zasíláte svým zákazníkům propagační e-maily či sms zprávy?

I tyto komunikační kanály a nástroje musí být nastavené v souladu s GDPR a příslušnými právními předpisy.

Facebook – jde o veřejně sdílenou sociální síť, kde i přes nastavení soukromí Vašeho účtu je nutné se v tomto prostředí chovat velmi opatrně, aby nedošlo k žádnému zneužití či úniku osobních údajů. Nedoporučujeme tedy vkládat do příspěvků či zpráv žádné citlivé osobní údaje o Vás či jiných osobách.

Osobní webová stránky – zde je nutné si ověřit, zda provozovatel domény má tuto doménu a servery zabezpečené. Další zásadou je nenutit psát zákazníky na tuto stránku údaje, které se pak ukládají na server. Tomuto můžete předejít tím, že zvolíte možnost kontaktního formuláře, zákazník Vám napíše, že má zájem o Vaše služby a Vy jej můžete přesměrovat přímo na zabezpečený e-shop MEDICALELIX. Stále platí, že každá osobní webová stránka poradce MEDICALELIX musí být schválena k provozu vedením MEDICALELIX.

SMS zprávy s reklamou či upozorněním na platnosti akcí – pokud se rozhodnete rozesílat vlastní SMS zprávy, musí s tím Váš zákazník předem souhlasit (nejlépe písemně), aby nedošlo k nepovolenému obtěžování zprávami. Pokud používáte k rozesílání hromadných zpráv speciální program, je nutné si u výrobce programu ověřit, že vložená telefonní čísla jsou v bezpečí a podniknout i další kroky k zabezpečení všech vložených telefonních čísel. Dále musíte aktivně reagovat na případné zpětné vazby, kdy zákazník odmítá zasílání dalších zpráv – ihned takové číslo z databáze pro zasílání SMS smažte. Tím se vyhnete možnému postihu ze strany Úřadu pro ochranu osobních údajů.

Propagační hromadné e-maily – komunikace je řízená přes speciální portály, kde je potřeba si uvědomit, že Vy jste objednatel služby, kterou Vám poskytuje cizí třetí (3.) subjekt. Svěřujete tedy OÚ Vašich zákazníků do rukou tohoto subjektu, a je nutné si ověřit, že i tento subjekt má dostatečné zabezpečení ochrany osobních údajů. V případě úniku OÚ by totiž mohl čekat postih i Vás, protože jste si nezajistili dostatečně zabezpečeného provozovatele služby.

Natáčíte videa, pořizujete fotografie se svými zákazníky a vystavujete je na veřejně dostupných kanálech?

V případě, že v rámci Vaší práce poradce pořizujete videozáznamy či fotografie s Vašimi zákazníky, které následně používáte pro propagační účely, či je jen vyvěšujete na veřejně dostupných informačních kanálech (sociální sítě, osobní internetové stránky, aj.), je nutné od zákazníka získat souhlas s pořízením fotografie či videozáznamu, výslovně jej seznámit s tím, k jakým účelům jsou fotografie a videa pořizovány a jak s nimi bude naloženo a současně upozornit zákazníka na možnost kdykoliv svůj souhlas odvolat a sdělit, jakým způsobem je možné provést odvolání souhlasu.

Např. Natáčíte video ze školení novinek MEDICALELIX, které chcete následně pověsit na Vaši osobní webovou stránku. Pro začátek doporučujeme ihned na začátku takového školení dát všem účastníkům k podpisu souhlas se zpracováním OÚ, resp. s pořízením fotografií či videozáznamů, kde bude napsáno, že v rámci školení budete pořizovat videozáznam (nebo fotografie) a jak budou OÚ účastníků zpracovány. Pokud Vám všichni účastníci tento souhlas podepíší, můžete videozáznam či fotografie pořídít a pracovat s nimi dále dle ujednání souhlasu. Pokud někdo souhlas nepodepíše je nutné při pořizování záznamu tohoto účastníka vynechat a zajistit, aby tato osoba nebyla nikde viditelná.

Zároveň je potřeba dát všem možnost svůj souhlas se zpracováním OÚ, resp. s pořízením videozáznamu či fotografie odvolat. V tomto případě budete muset zajistit odstranění této osoby ze záznamu či fotografie, nebo její zneviditelnění.

Na závěr

Pravidla a zásady plynoucí z nařízení (EU) 2016/679 (GDPR), ale i z ostatních právních předpisů je důležité v rámci fungování FKP systému MEDICALELIX dodržovat a se svěřenými osobními údaji zacházet v souladu s těmito pravidly a právními předpisy. Porušení jakékoliv zásady či právního předpisu může vést k bezpečnostnímu riziku, které by mohlo zapříčinit rozvázání obchodní spolupráce či uložení sankce.

Tento dokument platí ve znění uvedeném na internetových stránkách www.medicalex.cz provozovaných společností RP CLASS s.r.o., se sídlem Světová 523/1, Praha 8, 180 00

IČ: 174 92 092. Tento dokument nabývá platnosti a účinnosti 1. 9. 2022.

Změny v dokumentu vyhrazeny.