Definice pojmů dle GDPR

Pro účely nařízení GDPR se rozumí:

- **Subjekt údajů** - identifikovaná nebo identifikovatelná fyzická osoba
- **Osobní údaje** - veškeré informace o subjektu údajů, který lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
- **Zpracování** - jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
- **Omezení zpracování** - označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu
- **Profilování** - jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu
- **Pseudonymizace** - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě
- **Evidence** - jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska
- **Správce** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení
- **Zpracovatel** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
- **Příjemce** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují. Zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování
- **Třetí strana** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů
- **Souhlas** - subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů

- **Porušení zabezpečení osobních údajů** - porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů
- **Genetické údaje** - osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby
- **Biometrické údaje** - osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje
- **Údaje o zdravotním stavu** - osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu
- **Hlavní provozovna**:

a) v případě správce s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, ledaže jsou rozhodnutí o účelech a prostředcích zpracování osobních údajů přijímána v jiné provozovně správce v Unii a tato jiná provozovna má pravomoc vymáhat provádění těchto rozhodnutí, přičemž v takovém případě je za hlavní provozovnu považována provozovna, která tato rozhodnutí přijala

b) v případě zpracovatele s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, nebo pokud zpracovatel nemá v Unii žádnou ústřední správu, pak ta provozovna zpracovatele v Unii, kde probíhají hlavní činnosti zpracování v souvislosti s činnostmi provozovny zpracovatele, v rozsahu, v jakém se na zpracovatele vztahují specifické povinnosti podle tohoto nařízení

- **Zástupce** - jakákoli fyzická nebo právnická osoba usazená v Unii, která je správcem nebo zpracovatelem určena písemně podle článku 27 k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu tohoto nařízení
- **Podnik** - jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost
- **Skupina podniků** - skupina zahrnující řídící podnik a jím řízené podniky
- **Závazná podniková pravidla** - koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost
- **Dozorový úřad** - nezávislý orgán veřejné moci zřízený členským státem (ÚOOÚ)
- **Dotčený dozorový úřad** - dozorový úřad, kterého se zpracování osobních údajů dotýká, neboť:

a) správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu

b) subjekty údajů s bydlištěm v členském státě tohoto dozorového úřadu jsou nebo pravděpodobně budou zpracováním podstatně dotčeny, nebo

c) u něj byla podána stížnost

- **Přeshraničním zpracování** - buď:

a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě, nebo

b) zpracování osobních údajů, které probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě

- **Relevantní a odůvodněná námitka** - námitka vůči návrhu rozhodnutí za účelem posouzení, zda došlo k porušení tohoto nařízení, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s tímto nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie
- **Mezinárodní organizace** - organizace a jí podřízené subjekty podléhající mezinárodnímu právu veřejnému nebo jiný subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě

5. Oprávněný zájem je jeden z právních titulů, na základě kterého lze zpracovávat osobní údaje. Oprávněný zájem může vzniknout 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. Oprávněným zájmem dotčeného správce údajů je rovněž zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům. Rovněž tak zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu.
Tento právní titul by se neměl vztahovat na zpracování prováděné orgány veřejné moci při plnění jejich úkolů.

6. Životně důležitý zájem – Je možné jej použít pouze v omezeném okruhu případů a to, když je nutné zpracovat osobní údaje za účelem předejití vzniku ohrožení a újmy na životě subjektu údajů nebo jiné fyzické osoby. Typickým příkladem z praxe je, když je do nemocnice přivezen těžce zraněný pacient v bezvědomí, který není schopen dát souhlas se zpracováním svých osobních údajů. Použije se tedy právní titul životně důležitého zájmu, na základě kterého jsou osobní údaje zpracovány.

7. Souhlas se zpracováním osobních údajů musí být:

- **Prokazatelný** - správce osobních údajů nese důkazní břemeno ohledně udělení souhlasu, tzn. musí využít dostupných prostředků k ověření pravosti souhlasu, aby byl schopen tento souhlas prokázat. V případě e-mailů je takovým technickým řešením zaslání ověřovacího e-mailu na uvedenou adresu s odkazem pro potvrzení, zvané double opt-in nebo také confirmed opt-in. Často se lze setkat s názorem, že GDPR, ani zákon o některých službách informační společnosti o double opt-inu nikde nehovoří, ale to je zcela mylný výklad - jedná se o obecné právní předpisy, které musí fungovat nejen pro e-maily, a tak by vyjmenovávání konkrétních technických řešení bylo principiálně špatné. Nutnost double opt-inu vyplývá z důkazního břemene a faktu, že se jedná o jedinou metodu, jak vytvořit vazbu mezi zadanými údaji a e-mailovou adresou. Všechny ostatní metody jako např. Re-Captcha, checkboxy, opakované zadání, atp. chrání jen před automatizovaným zadáním a mohou zaznamenat pouze údaje o vyplnění údajů, nikoliv o souhlasu vlastníka e-mailové adresy.
- **Dobrovolný** - dobrovolnost nebo také nepodmíněnost je reakcí na častou praxi, kdy docházelo ke spojování a podmiňování souhlasů. Vznikaly tak situace, kdy nebylo možné provést nákup bez potvrzení zcela abstraktního souhlasu se zpracováním osobních údajů. Navíc tyto souhlasy byly často skryté, a tak se často jednalo o souhlas se všeobecnými obchodními podmínkami, ve kterých pak byl někde hluboko zakotven souhlas se zpracováním osobních údajů a zasíláním obchodních sdělení. Vzhledem k tomu, že GDPR silně cílí na transparentnost, tak je toto pochopitelně zcela nepřípustné.

- **Jednoznačný v účelu a rozsahu** - tento bod se také vztahuje k praxi rozsáhlých všeobecných podmínek a nedostatečné transparentnosti. Nově tak musí být zcela jasné, za jakým účelem osobní údaje poskytujete (proč) a v jakém rozsahu budou zpracovávány (k čemu). Tzn. pokud poskytnete souhlas čistě se zasíláním obchodních sdělení a zpracováním osobních údajů za tímto účelem a poskytnete pouze svou e-mailovou adresu, znamená to, že správce může použít pro zasílání obchodních sdělení pouze tento údaj. Aby vám však mohl posílat např. personalizované zprávy podle toho, jaké produkty si prohlédnete na jeho stránkách, musí mít váš souhlas i k tomuto.
- **Jednoznačný projev vůle** – podobně jako v současnosti také podle GDPR platí, že souhlas musí být udělen jednoznačným projevem vůle osoby. Z tohoto projevu musí být zjevné, že osoba skutečně chtěla udělit souhlas se zpracováním osobních údajů, nikoli že pouze vyjadřovala souhlas s obchodními podmínkami, uzavřením smlouvy, popř. že pouze nevyjádřila nesouhlas.
- **Informovaný** - toto platí i dnes. GDPR specifikuje, že subjekt, který uděluje souhlas, musí vědět, komu konkrétně tento souhlas uděluje, a být informován o účelu a rozsahu zpracování. Což v praxi znamená, že musí být uvedeno označení konkrétního správce a zpracovatelů, kteří budou mít přístup k osobním údajům, a jak konkrétně budou data použita. Zvláštní důraz je pak kladen na upozornění na jakékoliv zpracování probíhající mimo území EU. V případě souhlasu se zasíláním obchodních sdělení to znamená, že subjekt (příjemce) bude vědět, kdo mu bude co posílat. Tzn. obecné formulace typu “souhlasím s předáním údajů třetím stranám” v žádném případě nejsou přípustné a tyto třetí strany by měly být vyjmenované. Ačkoliv taková povinnost neplyne přímo z GDPR, je její splnění vyžadováno dozorovými orgány v zájmu zajištění informovanosti subjektu. Zvláště v případě využívání cloudových služeb je nutné dát pozor na to, že data mohou opustit EU. Není také přípustné, aby tyto informace byly skryté ve všeobecných podmínkách - naopak GDPR vyžaduje, aby byly dostupné a jasně pochopitelné.

8. výslovný souhlas

Už jsme zmínili, že **souhlas**, který vám zákazník ke zpracování svých osobních údajů pro marketingové účely poskytne, musí být výslovný. GDPR ale specifikuje ještě další požadavky: souhlas musí být **poskytnutý svobodně** a **jednoznačně**.

Co to v praxi znamená? GDPR naštěstí v konkrétní specifikaci nemlčí. Může se jednat například o:

- zaškrtnutí políčka (souhlasu) se zpracováním osobních údajů při návštěvě webových stránek,
- výběr technického nastavení služby,
- nebo jiné prohlášení či jednání, které jasně prokáže, že zákazník přijal navrhované zpracování jeho osobních údajů.

Jako souhlas ale nemůže být chápáno „mlčení“ zákazníka (v tomto ohledu opravdu neplatí, že mlčení je souhlas). Vyhněte se také předem zaškrtnutému políčku ve formuláři.

Pokud potřebujete souhlas ke zpracování osobních údajů pro více účelů, musí vám zákazník udělit souhlas pro všechny z nich. Proto je specifikujte.

A jakmile vám zákazník svůj souhlas udělí, nezapomeňte ho **evidovat**. Podle GDPR je totiž nutné souhlas zaznamenat a uchovat, a to včetně jména a data poskytnutí souhlasu. Tyto informace můžete v případě pochybností nebo konfliktu s úřady použít jako důkaz.